(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 762 338 A2

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
12.03.1997 Patentblatt 1997/11

(51) Int. Cl.[6]: **G07B 17/04**

(21) Anmeldenummer: **96250192.0**

(22) Anmeldetag: **06.09.1996**

(84) Benannte Vertragsstaaten:
CH DE FR GB IT LI

(30) Priorität: **08.09.1995 DE 19534530**

(71) Anmelder: **Francotyp-Postalia Aktiengesellschaft & Co.**
16547 Birkenwerder (DE)

(72) Erfinder:
- **Berthold, Arndt**
  10369 Berlin (DE)
- **Zarges, Olav A.**
  13353 Berlin (DE)

(54) Verfahren zur Absicherung von Daten und Programmcode einer elektronischen Frankiermaschine

(57) Die Erfindung betrifft ein Verfahren zur Absicherung von Daten und Programmcode einer elektronischen Frankiermaschine gegen Manipulation mit einem Mikroprozessor in einer Steuereinheit der Frankiermaschine zur Ausführung von Schritten für eine Start- und Initialisierungsroutine und nachfolgender Systemroutine mit einer Möglichkeit in einen Kommunikationsmodus mit einer entfernten Datenzentrale einzutreten sowie weiteren Eingabeschritten, um in einen Frankiermodus einzutreten von dem nach Ausführung einer Abrechnungs- und Druckroutine in die Systemroutine zurückverzweigt wird, umfassend

a) eine Startsicherheitsüberprüfung (1020) im Rahmen einer Start- und Initialisierungsroutine (101) vor einer sicheren Druckdatenaufrufroutine (1040) und der nachfolgenden Systemroutine (200) zur Feststellung der Gültigkeit eines Programm-Codes und/oder von Daten im vorbestimmten Speicherplatz und eines zugehörigen MAC (MESSAGE AUTHENTIFICATION CODE), welche im selben Speichermittel gespeichert vorliegen, wobei die Überprüfung auf gültigen Programm-Code und/oder auf Gültigkeit der Daten mittels eines ausgewählten Prüfsummenverfahrens innerhalb eines OTP-Prozessors (ONE TIME PROGRAMMABLE) durchgeführt wird, der intern die entsprechenden Programmteile enthält und

b) eine Überführung der Frankiermaschine in die vorgenannte Systemroutine (200) bei Gültigkeit der Daten oder Überführung der Frankiermaschine in einen ersten Modus, wenn die Daten ungültig sind bzw. ein spezifisches Manipulationskriterium erfüllt ist, durch Schritte zum Verhindern des Frankierens bzw. Sperrens der Frankiermaschine (1030) und/oder Schritte zum Verhindern einer weiteren Programmausführung bzw. einer vom OTP-Prozessor nach extern führenden Programmverzweigung im Rahmen vorgenannter Systemroutine (200).

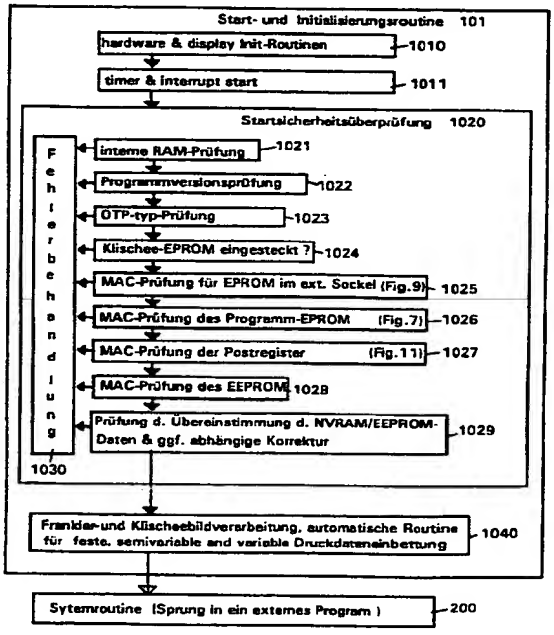

Fig. 4

EP 0 762 338 A2

BNSDOCID: <EP_____0762338A2_I_>

Beschreibung

Die Erfindung betrifft ein Verfahren zur Absicherung von Daten und Programmcode einer elektronischen Frankiermaschine in der im Oberbegriff des Anspruchs 1 bzw. 13 angegebenen Art. Dieses Verfahren verbessert die Sicherheit von Frankiermaschinen.

Eine Frankiermaschine erzeugt in der Regel einen Aufdruck in einer mit der Post vereinbarten Form rechtsbündig, parallel zur oberen Kante des Postgutes beginnend mit dem Inhalt Postwert im Poststempel, Datum im Tagesstempel und Stempelabdrucke für Werbeklischee und ggf. Sendungsart im Wahldruckstempel. Der Postwert, das Datum und die Sendungsart bilden hierbei die entsprechend dem Poststück einzugebenden variablen Informationen.

Beim Postwert handelt es sich meist um die vom Absender vorausbezahlte Beförderungsgebühr (Franko), die einen wiederauffüllbaren Guthabenregister entnommen und zum Freimachen der Postsendung verwendet wird. Im Gegensatz dazu wird beim Kontokorrentverfahren ein Register in Abhängigkeit von den mit dem Postwert vorgenommenen Frankierungen lediglich hochgezählt und in regelmäßigen Abständen, von einem Postinspektor abgelesen.

Grundsätzlich ist jede vorgenommene Frankierung abzurechnen und jede Manipulation, welche zu einer nichtabgerechneten Frankierung führt, muß verhindert werden.

Eine bekannte Frankiermaschine ist mit mindestens einem Eingabemittel, einem Ausgabemittel, einem Ein/Ausgabe-Steuermodul, einer Programm-, Daten- und insbesondere die Abrechnungsregister tragenden Speichereinrichtung, einer Steuereinrichtung und einem Druckermodul ausgerüstet. Bei einem Druckermodul mit Druckmechanik müssen auch Maßnahmen ergriffen werden, damit im ausgeschalteten Zustand die Druckmechanik nicht für unabgerechnete Abdrucke mißbraucht werden kann.

Die Erfindung betrifft insbesondere Frankiermaschinen, die einen vollelektronischen erzeugten Abdruck zum Frankieren von Postgut einschließlich Abdruck eines Werbeklischees liefern. Das hat zur Folge, daß nur noch im eingeschalteten Zustand ein nicht abgerechnetes gültiges Frankieren verhindert werden muß.

Bei einer aus der US 4 746 234 bekannten Frankiermaschine werden feste und variable Informationen in Speichermitteln (ROM, RAM) gespeichert, um diese dann, wenn ein Brief auf dem Transportpfad vor der Druckposition einen Mikroschalter betätigt, mittels eines Mikroprozessors auszulesen und um ein Drucksteuersignal zu bilden. Beide sind danach elektronisch zu einem Druckbild zusammengesetzt und können durch Thermotransferdruckmittel auf einen zu frankierenden Briefumschlag ausgedruckt werden.

Es wurde auch bereits ein Verfahren zum Steuern des spaltenweisen Druckens eines Postwertzeichenbildes in einer Frankiermaschine vorgeschlagen EP 578 042 A2, welches getrennt voneinander in graphische Pixelbilddaten umgesetzte feste und variable Daten während des spaltenweisen Druckens zusammensetzt. Es wäre daher schwierig, ohne großen und teuren Aufwand eine Manipulation am Drucksteuersignal vorzunehmen, wenn das Drucken mit einer hohen Geschwindigkeit erfolgt.

In üblicher Weise umfaßt die Speichereinrichtung mindestens einen nichtflüchtigen Speicherbaustein, der das aktuell verbliebene Restguthaben enthält, welches daraus resultiert, daß von einem früher in die Frankiermaschine geladenen Guthaben der jeweilige zu drukkenden Portowert abgezogen wird. Die Frankiermaschine blockiert, wenn das Restguthaben Null ist.

Bekannte Frankiermaschinen enthalten in mindestens einem Speicher drei relevante Postregister für verbrauchten Summenwert (steigendes Register), noch verfügbares Restguthaben (fallendes Register) und Register für eine Kontrollsumme. Die Kontrollsumme wird mit der Summe aus verbrauchten Summenwert und aus verfügbaren Guthaben verglichen. Bereits damit ist eine Überprüfung auf richtige Abrechnung möglich.

Weiterhin ist es auch möglich von einer Datenzentrale über eine Fernwertvorgabe eine Wiederaufladeinformation zur die Frankiermaschine zu übertragen, um in das Register für das Restguthaben (Restwert) ein Guthaben nachzuladen. Es versteht sich von selbst, daß hierfür geeignete Sicherheitsmaßnahmen getroffen werden müssen, damit das in der Frankiermaschine gespeicherte Guthaben nicht in unbefugter Art und Weise aufgestockt werden kann. Die vorgenannten Lösungen gegen Mißbrauch und Fälschungsversuche zu schützen, erfordert einen zusätzlichen materiellen und zeitlichen Aufwand.

Aus der US 4 864 506 ist bekannt, daß eine Kommunikation zur entfernten Datenzentrale von der Frankiermaschine aufgenommen wird, wenn der Wert des Guthabens im fallenden Register unter einem Schwellwert liegt und eine vorbestimmte Zeit erreicht ist.

Aus obengenanntem Patent ist weiterhin bekannt, daß die Datenzentrale zum Empfang von Registerdaten und zur Kontrolle, ob die Frankiermaschine noch an eine bestimmte Telefonnummer angeschlossen ist - die Verbindung mit der Frankiermaschine nach einer definierten Zeitdauer aufnimmt und die Frankiermaschine nur zu vorbestimmten Zeiten antwortet.

Es ist nach obengenanntem Patent außerdem vorgesehen, vor einer Guthabennachladung in die Frankiermaschine, zur Autorisierung durch die Datenzentrale die Identitätsnummer der Frankiermaschine und die Werte im fallenden und steigenden Register abzufragen.

Weiterhin ist aus obengenanntem Patent bekannt, daß die Kommunikation der Datenzentrale mit der Frankiermaschine nicht auf bloße Guthabenübertragung in die Frankiermaschine beschränkt bleiben braucht. Vielmehr wird im Falle einer Abmeldung der Frankierma-

BNSDOCID <EP_____0762338A2_I_>

schine die Kommunikation der Datenzentrale mit der Frankiermaschine zur Übertragung des Restguthabens der Frankiermaschine in die Datenzentrale genutzt. Der Wert im fallenden Postregister der Frankiermaschine ist dann Null, was die Frankiermaschine wirksam außer Betrieb setzt.

Ein Sicherheitsgehäuse für Frankiermaschinen, welches innere Sensoren aufweist, ist aus der DE 41 29 302 A1 bekannt. Die Sensoren sind insbesondere mit einer Batterie verbundene Schalter, welche beim Öffnen des Sicherheitsgehäuses aktiv werden, um einen das Restwertguthaben speichernden Speicher (fallendes Postregister) durch Unterbrechen der Energiezufuhr zu löschen. Es ist bekanntlich aber nicht vorhersagbar, welchen Zustand ein spannungsloser Speicherbaustein beim Wiederkehr der Spannung einnimmt. Somit könnte auch ein nicht bezahltes höheres Restguthaben entstehen. Andererseits kann nicht ausgeschlossen werden, daß sich auf oben genannte Weise, das Restwertguthaben zumindest teilweise entlädt. Das wäre aber bei einer Inspektion nachteilig, da das Restwertguthaben, welches vom Frankiermaschinennutzer bezahlt worden war, auch wieder geladen werden muß, die Höhe dieses Restguthabens jedoch durch o.g. Einflüsse verfälscht sein kann. Schließlich ist der Beschreibung nicht entnehmbar, wie verhindert werden kann, daß ein Manipulator ein nicht bezahltes Restguthaben wieder herstellt.

Bei bekannten Frankiermaschinen sind bereits weitere Sicherheitsmaßnahmen wie Wegbrechschrauben und gekapseltes abgeschirmtes Sicherheitsgehäuse bekannt. Üblich sind auch Schlüssel und ein Zahlenschloß um den Zugriff auf die Frankiermaschine zu erschweren.

In der US 4 812 994 soll ein unautorisierter Zugriff einer Benutzung der Frankiermaschine darüber hinaus durch Sperrung der Frankiermaschine bei Falscheingabe eines vorbestimmten Paßwortes verhindert werden.

Außerdem kann die Frankiermaschine mittels Paßwort und entsprechender Eingabe über Tastatur so eingestellt werden, daß ein Frankieren nur während eines vorbestimmten Zeitintervalls bzw. Tageszeiten möglich ist.

Das Paßwort kann durch einen Personalcomputer über MODEM, durch eine Chipkarte oder manuell in die Frankiermaschine eingegeben werden. Nach positiven Vergleich mit einem in der Frankiermaschine gespeicherten Paßwort wird die Frankiermaschine freigegeben. Im Steuermodul der Abrechnungseinheit ist ein Sicherheitsmodul (EPROM) integriert. Als weitere Sicherheitsmaßnahme ist ein Verschlüsselungsmodul (separater Mikroprozessor oder Programm für FM-CPU basierend auf DES- oder RSA-Code) vorgesehen, der eine den Portowert, die Teilnehmernummer, eine Transaktionsnummer und ähnliches umfassende Erkennungsnummer im Frankierstempel erzeugt. Bei genügend krimineller Energie könnte aber auch ein Paßwort ausgeforscht und samt Frankiermaschine in den Besitz eines Manipulators gebracht werden.

Es ist bereits in der US 4,812,965 ein Ferninspektionssystem für Frankiermaschinen vorgeschlagen worden, welches auf speziellen Mitteilungen im Abdruck von Poststücken, die der Zentrale zugesandt werden müssen, oder auf einer Fernabfrage über MODEM basiert. Sensoren innerhalb der Frankiermaschine sollen jede vorgenommene Verfälschungshandlung detektieren, damit in zugehörigen Speichern ein Flag gesetzt werden kann, falls in die Frankiermaschine zu Manipulationszwecken eingegriffen wurde. Ein solcher Eingriff könnte erfolgen, um ein nicht bezahltes Guthaben in die Register zu laden.

Bei Feststellung einer Manipulation wird die Frankiermaschine während der Ferninspektion über Modem durch ein von der Datenzentrale ausgehendes Signal gesperrt. Eine geschickte Manipulation könnte aber andererseits darin bestehen, nach der Herstellung von nicht abgerechneten Frankieraufdrucken, das Flag und die Register in den ursprünglichen Zustand zurückzuversetzen. Eine solche Manipulation wäre über Ferninspektion durch die Datenzentrale nicht erkennbar, wenn diese rückgängig gemachte Manipulation vor der Ferninspektion lag. Auch der Empfang der Postkarte von der Datenzentrale, auf welche eine zu Inspektionszwecken vorzunehmende Frankierung erfolgen soll, gestattet dem Manipulator die Frankiermaschine in ausreichender Zeit in den ursprünglichen Zustand zurückzuversetzen. Damit ist also noch keine höhere Sicherheit erreichbar.

Der Nachteil eines solchen Systems besteht darin, daß nicht verhindert werden kann, daß ein genügend qualifizierter Manipulator, welcher in die Frankiermaschine einbricht, seine hinterlassenen Spuren nachträglich beseitigt, indem die Flags gelöscht werden. Auch kann damit nicht verhindert werden, daß der Abdruck selbst manipuliert wird, welcher von einer ordnungsgemäß betriebenen Maschine hergestellt wird. Bei bekannten Maschinen besteht die Möglichkeit, einer Herstellung von Abdrucken mit dem Portowert Null. Derartige Nullfrankierungen werden zu Testzwecken benötigt, und könnten auch nachträglich gefälscht werden, indem ein Portowert größer Null vorgetäuscht wird.

Ein Sicherheitsabdruck gemäß der FP-eigenen europäische Patentanmeldung EP 576 113 A2 sieht Symbole in einem Markierungsfeld im Frankierstempel vor, die eine kryptifizierte Information enthalten. Dies gestattet der Postbehörde, welche mit der Datenzentrale zusammenwirkt, aus dem jeweiligem Sicherheitsabdruck eine Erkennung einer Manipulation an der Frankiermaschine zu beliebigen Zeitpunkten. Zwar ist eine laufende Kontrolle solcher mit einem Sicherheitsabdruck versehenen Poststücke über entsprechende Sicherheitsmarkierungen im Stempelbild technisch möglich, jedoch bedeutet das einen zusätzlichen Aufwand im Postamt. Bei einer auf Stichproben beruhenden Kontrolle, wird aber eine Manipulation in der Regel erst spät festgestellt.

Andererseits kann im Datenzentrum eine zusätzli-

BNSDOCID: <EP_____0762338A2_I_>

che Auswertung hinsichtlich eines Nutzers einer Frankiermaschine, die vom Nutzer über das Inspektionsdatum hinaus weiterbetrieben wurde, erfolgen. Jedoch kann bisher aus diesen Informationen noch nicht eine in Fälschungsabsicht vorgenommene Manipulation geschlußfolgert werden.

In der US 4 251 874 wird ein mechanisches Druckwerk, das zum Drucken voreingestellt werden muß, mit einer Detektoreinrichtung verwendet, um die Voreinstellung zu überwachen. Ferner sind im elektronischen Abrechnungssystem Mittel zum Feststellen von Fehlern in Daten- und Steuersignalen vorgesehen. Erreicht diese Fehlerzahl einen vorgegebenen Wert, wird der weitere Betrieb der Frankiermaschine unterbrochen. Der plötzliche Ausfall der Frankiermaschine ist aber für den Frankiermaschinenbenutzer nachteilig. Bei einem nichtmechanischen Druckprinzip sind andererseits kaum solche internen Fehler zu erwarten und bei einem schweren Fehler ist die Frankiermaschine ohnehin sowieso sofort abzuschalten. Außerdem wird die Sicherheit gegenüber einer Manipulation der Frankiermaschine dadurch kaum größer, indem die Frankiermaschine nach einer vorbestimmten Fehleranzahl abgeschaltet wird.

Aus der US 4 785 417 ist eine Frankiermaschine mit einer Programmsequenzüberwachung bekannt. Der korrekte Ablauf eines größeren Programmstücks wird mittels eines jedem Programmteil zugeordneten speziellen Codes kontrolliert, der bei Aufruf des Programmstücks in einer bestimmten Speicherzelle im RAM abgelegt wird. Es wird nun überprüft, ob der in der vorgenannten Speicherzelle abgelegte Code im gerade ablaufenden Programmteil immer noch vorhanden ist. Würde bei einer Manipulation der Lauf eines Programmteils unterbrochen und ein anderer Programmteil läuft ab, kann durch eine solche Kontrollfrage ein Fehler festgestellt werden. Eine solche Überwachung auf Ausführung aller Programmteile beruht auf der Verschiedenheit der Code, wobei bei einer sehr hohen Anzahl an Programmteilen auch die Länge des Codewortes entsprechend größer sein muß. Ein Vergleich solcher Codewörter ist natürlich zeitintensiver was für schnelle Frankiermaschinen einen Kostenmehraufwand für einen schnelleren Prozessor verursacht. Bei einer Manipulation mittels solcher fehlerfreien Programmteile aus der Frankiermaschine, welche zu einem manipulierten Programmstück zusammengesetzt wurden, würde kein Fehler festgestellt werden, da bei Programmverzweigungen nicht festgestellt werden kann, welcher Programmzweig wie oft durchlaufen wurde.

Eine andere Art einer erwarteten Manipulation ist das Nachladen der Frankiermaschinenregister mit einem nicht abgerechneten Guthabenwert. Damit ergibt sich das Erfordernis einer gesicherten Nachladung. Eine zusätzliche Sicherheitsmaßnahme ist nach US 4 549 281 der Vergleich einer internen in einem nichtflüchtigen Register gespeicherten festen Kombination mit einer eingegebenen externen Kombination, wobei nach einer Anzahl an Fehlversuchen, d.h. Nichtidentität der Kombinationen, die Frankiermaschine mittels einer Hemmungselektronik gesperrt wird. Nach US 4 835 697 kann zur Verhinderung eines unautorisierten Zugriffs auf die Frankiermaschine die Kombination grundsätzlich gewechselt werden. Aus der US 5,077,660 ist außerdem eine Methode zum Wechsel der Konfiguration der Frankiermaschine bekannt, wobei die Frankiermaschine mittels geeigneter Eingabe über eine Tastatur vom Betriebsmode in einen Konfigurationsmode umgeschaltet und eine neue Metertypnummer eingegeben werden kann, welche der gewünschten Anzahl an Merkmalen entspricht. Die Frankiermaschine generiert einen Code für die Kommunikation mit dem Computer der Datenzentrale und die Eingabe der Identifikationsdaten und der neuen Metertypnummer in vorgenannten Computer, der ebenfalls einen entsprechenden Code zur Übermittlung und Eingabe in die Frankiermaschine generiert, in der beide Code verglichen werden. Bei Übereinstimmung beider Code wird die Frankiermaschine konfiguriert und in den Betriebsmode umgeschaltet. Die Datenzentrale hat dadurch vom jeweils eingestellten Metertyp für die entsprechende Frankiermaschine immer genaue Aufzeichnungen. Jedoch ist die Sicherheit allein von der Verschlüsselung der übertragenen Code abhängig.

Darüber hinaus ist aus der EP 388 840 A2 eine vergleichbare Sicherheitstechnik für ein Setzen einer Frankiermaschine bekannt, um diese von Daten zu säubern, ohne daß die Frankiermaschine zur Herstellerfirma transportiert werden muß. Auch hier ist die Sicherheit allein von der Verschlüsselung der übertragenen Code abhängig.

Die gesicherte Nachladung einer Frankiermaschine mit einem Guthaben wurde in US 3 255 439 einerseits bereits mit einer automatischen Signalübertragung von der Frankiermaschine zur Datenzentrale verbunden, wenn immer eine vorbestimmte Geldmittelsumme, welche frankiert wurde, oder Stückzahl an bearbeiteten Poststücken oder eine vorbestimmte Zeitperiode erreicht wurde. Alternativ kann ein der Geldmittelsumme, Stückzahl oder Zeitperiode entsprechendes Signal übermittelt werden. Dabei erfolgt die Kommunikation mittels binärer Signale über miteinander über eine Telefonleitung verbundene Konverter. Die Maschine erhält eine ebenso gesicherte Nachladung entsprechend der Kreditbalance und blockiert in dem Fall, wenn kein Kredit nachgeliefert wird.

Aus der US 4 811 234 ist bekannt, die Transaktionen verschlüsselt durchzuführen und dabei die Register der Frankiermaschine abzufragen und die Registerdaten der Datenzentrale zu übermitteln, um einen zeitlichen Bezug der Verringerung des im Register gespeicherten verfügungsberechtigten Betrages anzuzeigen. Einerseits identifiziert sich die Frankiermaschine bei der Datenzentrale, wenn ein voreinstellbarer Schwellwert erreicht ist, mittels ihres verschlüsselten Registerinhaltes. Andererseits modifiziert die Datenzentale durch entsprechende Berechtigungssignale den gewünschten Frankierbetrag, bis zu dem frankiert

BNSDOCID: <EP_____0762338A2_I_>

werden darf. Die Verschlüsselung ist somit die einzige Sicherheit gegen eine Manipulation der Registerstände. Wenn also ein Manipulator zwar ordnungsgemäß immer den gleichen Betrag in gleichen zeitlichen Intervallen lädt, aber zwischenzeitlich mit der manipulierten Frankiermaschine einen viel höheren Betrag frankiert, als er bezahlt hat, kann die Datenzentrale keine Manipulation feststellen.

Aus der EP 516 403 A2 ist bekannt, die in der Vergangenheit protokollierten und in einem Speicher gespeicherten Fehler der Frankiermaschine regelmäßig zu einem entfernten Fehleranalysecomputer zur Auswertung zu übertragen. Eine solche Ferninspektion erlaubt eine frühe Warnung vor einem auftretenden Fehler und ermöglicht weitere Maßnahmen (Service) zu ergreifen. Allein dies bietet noch kein ausreichendes Kriterium für eine Manipulation.

Gemäß der GB 22 33 937 A und US 5 181 245 kommuniziert die Frankiermaschine periodisch mit der Datenzentrale. Ein Blockiermittel gestattet die Frankiermaschine nach Ablauf einer vorbestimmten Zeit bzw. nach einer vorbestimmten Anzahl an Operationszyklen, zu blockieren und liefert eine Warnung an den Benutzer. Zum Freischalten muß von außen ein verschlüsselter Code eingegeben werden, welcher mit einem intern erzeugten verschlüsselten Code verglichen wird. Um zu verhindern, daß falsche Abrechnungsdaten an die Datenzentrale geliefert werden, werden in die Verschlüsselung des vorgenannten Codes die Abrechnungsdaten mit einbezogen. Nachteilig ist, daß die Warnung zugleich mit dem Blockieren der Frankiermaschine erfolgt, ohne daß der Benutzer eine Möglichkeit hat, sein Verhalten rechtzeitig entsprechend zu ändern.

Aus der US 5 243 654 ist eine Frankiermaschine bekannt, wo die laufenden von Uhr/Datumsbaustein gelieferten Zeitdaten mit gespeicherten Stillegungszeitdaten verglichen werden. Ist die gespeicherte Stillegungszeit durch die laufende Zeit erreicht, wird die Frankiermaschine deaktiviert, das heißt ein Drucken verhindert. Bei Verbindungsaufnahme mit einer Datenzentrale, welche die Abrechnungsdaten aus dem steigenden Register ausliest, wird der Frankiermaschine ein verschlüsselter Kombinationswert übermittelt und eine neue Frist gesetzt, wodurch die Frankiermaschine wieder betriebsfähig gemacht wird. Dabei ist der Verbrauchssummenbetrag, der das verbrauchte Porto summiert enthält und von der Datenzentrale gelesen wird, ebenfalls Bestandteil des verschlüsselt übermittelten Kombinationswertes. Nach der Entschlüsselung des Kombinationswertes wird der Verbrauchssummenbetrag abgetrennt und mit dem in der Frankiermaschine gespeicherten Verbrauchssummenbetrag verglichen. Ist der Vergleich positiv, wird die Sperre der Frankiermaschine automatisch aufgehoben. Durch diese Lösung wird erreicht, daß sich die Frankiermaschine bei der Datenzentrale periodisch meldet, um Abrechnungsdaten zu übermitteln. Es sind jedoch Benutzungsfälle durchaus denkbar, wo das zu frankierende Postaufkommen schwankt (Saisonbetrieb). In diesen Fällen würde in nachteiliger Weise die Frankiermaschine unnötig oft blockiert werden.

Es war die Aufgabe zu lösen, die Nachteile des Standes der Technik zu überwinden und einen signifikanten Zuwachs an Sicherheit ohne eine außerordentliche Inspektion vor Ort zu erreichen. Dabei soll ohne daß eine besondere mechanische Kapselung bzw. ohne daß ein Sensor zur Erkennung des geöffneten Gehäuses erforderlich ist, eine in Fälschungsabsicht vorgenommene Manipulation erkannt und die Datensicherheit erhöht werden. Das Sicherheitsgehäuse soll durch ein Gehäuse ersetzt werden, welches die Zugänglichkeit auf einzelne Bausteine der Elektronik für den Servicetechniker verbessert. Außerdem soll ein Prozessor ohne einen internen NV-RAM eingesetzt werden. Eine weitere Aufgabe ist es, die Sicherheit der Schlüssel in der Frankiermaschine zu verbessern, die bei einer Kommunikation mit dem Datenzentrum benötigt werden, wenn Daten übermittelt werden.

Die Aufgabe wird mit den kennzeichnenden Merkmalen des Anspruchs 1, 13 bzw. 14 gelöst.

Die Erfindung geht von einem Prozessor aus, der nur einmal programmiert werden kann.

Eine erhöhte Sicherheit kann beispielsweise mit einem maskenprogrammierten Mikroprozessor erreicht werden, der nach außen Port's und eine interne Busstruktur, ein internes ROM, ein internes RAM für sicherheitsrelevante Abläufe aufweist. In das interne Rom werden sicherheitsrelevante Daten und Routinen während der Herstellung eingebrannt.

Eine bevorzugte Variante geht von einer Frankiermaschine mit Mikroprozessor aus, in der Mikroprozessor einen internen ROM enthält der ein Auslesen des darin enthaltenen Programmcodes nicht erlaubt. Dies kann ein handelsüblicher OTP-Prozessor (ONE TIME PROGRAMMABLE) sein, den man nach dem Programmiervorgang durch setzen/brennen einer Auslesesperre in einen solchen Zustand versetzt.

Die Frankiermaschine kann auch mit einem OTP-Typ ausgerüstet werden, der ein Auslesen von sicherheitsrelevanten Daten und Programmen in verschlüsselter Form gestattet (Encryption-Table). Das hat den Vorteil, daß eine Kontrolle darüber möglich ist, ob die Daten ordnungsgemäß gespeichert wurden.

Die Erfindung hat den Vorteil, daß Programmcode und konstante sicherheitsrelevante Daten nicht verändert, nicht übersprungen und nicht ausgespäht werden können. Damit ist die Programmausführung von Programmteilen, die im internen OTP-ROM ausgeführt werden, nicht manipulierbar. Solange keine Programmverzweigung stattfindet besteht ein sicherer Schutz vor betrügerischer Manipulation. Erfindungsgemäß wird mit den Programmteilen, die im internen OTP-ROM ausgeführt sind, auch ein Schutz auch von extern gespeicherten Programmteilen ermöglicht, die beispielsweise in einem EPROM gespeichert vorliegen. Im OTP-ROM sind erfindungsgemäß auch eine Vielzahl von Schlüsseln und ein Verschlüsselungsalgorithmus gespeichert, welche bei der Programmausführung von sicherheitsre-

BNSDOCID: <EP_____0762338A2_I_>

levanten Transaktionen und bei der externen Speicherung von sicherheitsrelevanten Daten Anwendung finden.

Der EPROM nimmt den größeren Teil des Programmcodes auf und stellt dem Mikroprozessor über den Mikroprozessorbus einen externen Programmcode zur Verfügung. Da aber zusätzlich die Programmvariablen im internen OTP-RAM gespeichert werden, wird eine sicherheitsrelevante Kapselung der Programmausführung erreicht. Mit einem OTP-Prozessor lassen sich somit gezielt Programmausführungen in unterschiedlichen Sicherheitsstufen realisieren. Eine fehlerhafte oder manipulierte Frankiermaschine verbleibt mit ihrer Programmausführung vollständig im OTP-ROM und kann nicht in andere Betriebsmodi gezwungen werden.

Die erfindungsgemäße Lösung geht weiterhin davon aus, daß die in der Frankiermaschine gespeicherten Geldmittel vor unautorisiertem Zugriff geschützt werden müssen. Die Verfälschung von in der Frankiermaschine gespeicherten Daten wird so weit erschwert, daß sich der Aufwand für einen Manipulator nicht mehr lohnt.

Handelsübliche OTP-Prozessoren (ONE TIME PROGRAMMABLE) können alle sicherheitsrelevanten Programmteile im Inneren des Prozessorgehäuses enthalten, außerdem den Code zur Bildung des Message Authentification Code (MAC). Letzterer ist eine verschlüsselte Checksumme, die an eine Information angehängt wird. Als Kryptoalgorithmus ist beispielsweise Data Encryption Standard (DES) geeignet. Damit lassen sich MAC-Informationen an die sicherheitsrelevanten Registerdaten anhängen und somit die Schwierigkeit der Manipulation an den Postregistern maximal erhöhen.

Diese sicherheitsrelevanten Programmteile umfassen auch Programmteile für eine Flußkontrolle, die die Anzahl der abgelaufenen Programmteile überwacht. Damit können Fehlfunktionen des Mikroprozessors oder in Fälschungsabsicht vorgenommene Manipulationen aufgedeckt werden. Spezifische Rechenoperationen erlauben die Überprüfung, welche Programmteile wie oft benutzt wurden.

Eine andere Sicherheitsmaßnahme, die zusätzlich zum Error Handling (Kill Mode) der Startsicherheitsüberprüfung ablaufen kann, ist das Überwachen der Programmlaufzeit ausgewählter sicherheitsrelevanter Programme oder Programmteile in einem Time Supervisions Mode (Kill Mode 1). Bei Abweichung der Laufzeit von Programmen bzw. Programmteilen von einer vorbestimmten Laufzeit, wie sie bei Manipulation bzw. Überwachung des Programmablaufes mittels Emulator auftreten, wird die Maschine gehemmt. Ein solcher Programmteil betrifft den Kommunikationsmodus. Ein Geheimschlüssel für die verschlüsselte Kommunikation wird außerhalb des OTP in verschlüsselter Form gespeichert. Der OTP kann daraus den eigentlichen Schlüssel durch Entschüsselung zurückgewinnen, welcher für Transaktionen zwischen Frankiermaschine und Datenzentrale benötigt wird.

Die Frankiermaschine kann von der Systemroutine mittels eines Entscheidungskriteriums in den zweiten Modus eintreten, um an den Benutzer der Frankiermaschine eine Warnung und Aufforderung zur Kommunikation mit der Datenzentrale abzugeben. Gleichzeitig wird auch von der Datenzentrale das Verhalten des Frankiermaschinenbenutzers auf der Basis von bisherigen während einer Kommunikation übermittelten Daten überwacht.

In der Frankiermaschine ist vorgesehen, daß ein spezieller Sleepingmodezähler bei jeder Kommunikation mit der Datenzentrale auf eine spezifische Stückzahl gesetzt wird und bei jeder Frankierung, d.h. im Verlauf einer Abrechnungs- und Druckroutine, zur Weiterzählung veranlaßt wird, bis eine bestimmte Zahl erreicht wird. Die spezifische Stückzahl kann sowohl in der Frankiermaschine errechnet, als auch in der Datenzentrale errechnet und an die Frankiermaschine über eine Kommunikationsverbindung übermittelt werden.

Ausgehend von der Überlegung mit nur einem Mikroprozessor und einem geeigneten Programm einer Frankiermaschine ein Verfahren zur Verbesserung der Sicherheit von Frankiermaschinen zu schaffen, bildet eine gleichzeitig in der Datenzentrale identisch vorliegende nutzerspezifische Information über den Guthabenverbrauch eine erste Berechnungsbasis, um in der Datenzentrale gespeichert vorliegenden Guthabenverbrauchs- und Guthabennachladedatumsdaten auf ihre Plausibilität zu überprüfen. Eine weitere erfinderische Berechnungsbasis aufgrund weiterer Daten, insbesondere in Verbindung mit der Stückzahl seit der letzten Kommunikation, gestattet eine außerordentliche Inspektion derjenigen Frankiermaschine vor Ort vorzunehmen, welche bei der Datenzentrale als suspekt gilt.

Die Frankiermaschine, welche eine regelmäßige Guthabennachladung erhält und dabei inspiziert wird, kann dabei als unverdächtig eingestuft werden. Die über ein vorgegebenes Inspektionsdatum ohne Inspektion weiter betriebene Frankiermaschine, muß jedoch nicht zwangsläufig manipuliert sein. Vielmehr kann sich auch das von der Frankiermaschine zu bearbeitende Postaufkommen überdurchschnittlich verringert haben. Wenn in der Frankiermaschine noch genügend Restwertguthaben verfügbar ist, kann damit natürlich weiterfrankiert werden. Erst eine außerordentliche Inspektion vor Ort, kann in diesem Falle klären, ob eine Manipulation vorliegt.

Für die Überprüfung suspekter Frankiermaschinen wird von der Datenzentrale der Postbehörde bzw. dem mit der Prüfung beauftragten Institut die zugehörige Frankiermaschinenseriennummer übermittelt. Mit dieser Information kann das Vorkommen an Poststücken (Briefen) bestimmter Absender überwacht werden, indem deren Anzahl im Zeitintervall beispielsweise von 90 Tagen gezählt wird.

Bei einer Inspektion oder Reparatur bzw. durch den Service vor Ort muß eventuell in die Frankiermaschine eingegriffen werden. Zur Vorbereitung des Eingriffs werden die Register der Frankiermaschine abgefragt bzw.

BNSDOCID <EP_____0762338A2_I_>

ausgedruckt, um die Art des erforderlichen Eingriffs zu ermitteln. Nach einem erfolgten autorisierten Eingriff in die Frankiermaschine ist der ursprüngliche Betriebszustand mittels spezieller geeigneter Weise eingegebenen Daten wiederhergestellt.

Nimmt aber ein Manipulator einen unautorisierten Eingriff vor, wird die Frankiermaschine nach dem Einschalten durch das Überführen der Frankiermaschine in den ersten Modus (Error Handling) wirksam außer Betrieb gesetzt.

Eine andere Sicherheitsmaßnahme, die im zweiten Modus neben oder anstatt einer Sleeping-Mode-Variante durchgeführt werden kann, ist der Error Overflow Mode. Dieser verlängert die Reaktionszeitdauer der Frankiermaschine bei Überschreiten einer vorbestimmten Anzahl an Fehlern und meldet über die Anzeige diesen Zustand an den Bediener der Frankiermaschine. Wird der Zustand der Überschreitung der Fehleranzahl nicht beseitigt, beispielsweise im Rahmen einer Inspektion durch einen Servicedienst oder durch Rücksetzen während einer Kommunikation mit der Datenzentrale, kann die Reaktionszeitdauer weiter erhöht werden, um eventuelle Manipulationen zu erschweren.

Das Verfahren zur Absicherung von Daten und Programmcode einer elektronischen Frankiermaschine, welche zur Kommunikation mit einer entfernten Datenzentrale fähig ist und einen OTP-Prozessor in einer Steuereinrichtung der Frankiermaschine aufweist, umfaßt außerdem das Übertragen eines extern gespeicherten vorbestimmten MAC-Wert in den internen OTP-RAM und ein Bilden einer Checksumme im OTP-Prozessor über den Inhalt desjenigen externen Speichers, welchem der MAC zugeordnet ist, und einen Vergleich des Ergebnisses mit dem im internen OTP-RAM flüchtig gespeicherten vorbestimmten Wert des MAC vor und/oder nach Ablauf des Frankiermodus bzw. Betriebsmodus, und somit auch nach der Initialisierung (das heißt wenn die Frankiermaschine betrieben wird), oder in Zeiten, in welchen nicht gedruckt wird (das heißt wenn die Frankiermaschine im Standby-Modus betrieben wird). Im Fehlerfall erfolgt dann eine Protokollierung und anschließende Blockierung der Frankiermaschine.

Die Erfindung umfaßt weiterhin eine Durchführung von Authentizitätsprüfungen im Ergebnis der Druckdateneingabe für Rahmen und/oder Fensterdaten während der Start- und Initialisierungsroutine 101 und einer Eingabe-, Anzeige- und Prüfroutine für sicherheitsrelevante Fensterdaten welche bei der Druckdateneingabe geändert wurden. Bei fehlender Authentizität werden Schritte zum Verhindern einer weiteren Programmausführung bzw. einer vom OTP-Prozessor nach extern führenden Programmverzweigung im Rahmen vorgenannter Systemroutine. Bei bestehender Authentizität werden Schritte zur weiteren Programmausführung im Rahmen vorgenannter Systemroutine durchgeführt.

Erfindungsgemäß ist ein Verfahren vorgesehen, umfassend

a) eine Startsicherheitsüberprüfung im Rahmen einer Start- und Initialisierungsroutine, welche abläuft vor einer sicheren Druckdatenaufrufroutine und der nachfolgenden Systemroutine, zur Feststellung der Gültigkeit eines Programm-Codes und/oder von Daten im vorbestimmten Speicherplatz,

b) Überführung der Frankiermaschine in die vorgenannte Systemroutine bei Gültigkeit der Daten oder Überführung der Frankiermaschine in einen ersten Modus, wenn die Daten ungültig sind bzw. ein spezifisches Manipulationskriterium erfüllt ist,

c) kontinuierliche Programmüberwachung innerhalb der Systemroutine und Überführung der Frankiermaschine in den ersten Modus, wenn die Daten ungültig sind bzw. ein spezifisches Manipulationskriterium erfüllt ist, wobei über jeden der Subblöcke eines Blocks eine Prüfsumme oder MAC inkrementell berechnet wird, wobei eine kumulierte Prüfsumme bzw. MAC gebildet und ein Vergleich mit einem früher gespeicherten Wert für vorgenannte Prüfsumme bzw. MAC vorgenommen wird, um die Authentizität der Programmteile voranschreitend festzustellen.

Vorteilhafte Weiterbildungen der Erfindung sind in den Unteransprüchen gekennzeichnet bzw. werden nachstehend zusammen mit der Beschreibung der bevorzugten Ausführung der Erfindung anhand der Figuren näher dargestellt. Es zeigen:

Figur 1, Blockschaltbild einer Frankiermaschine mit erfindungsgemäß erhöhter Sicherheit,

Figur 2, Variante mit OTP in der Steuereinrichtung der Frankiermaschine,

Figur 3, Gesamtablaufplan für die Frankiermaschine nach der erfindungsgemäßen Lösung,

Figur 4, Ablaufplan für die Start- und Initialisierungsroutine,

Figur 5, Ablaufplan für den Frankiermodus,

Figur 6, Bilden einer MAC-Prüfsumme mittels Verschlüsselung für ein externes Programm-EPROM,

Figur 7, Ablaufplan zum Prüfen eines externen Programm-EPROM's,

Figur 8, Bilden einer MAC-Prüfsumme mittels Verschlüsselung für ein externes Klischee-EPROM,

Figur 9, Ablaufplan zum Prüfen eines externen Klischee-EPROM's,

BNSDOCID: <EP_____0762338A2_I_>

Figur 10, Ablaufplan zum Absichern ausgewählter Registerdaten,

Figur 11, Ablaufplan zum Prüfen ausgewählter Registerdaten,

Figur 12, Ablaufplan zur Eingabeverschlüsselung der Schlüssel, die für die gesicherte Übertragung von Daten zwischen Frankiermaschine und Datenzentrale eingesetzt werden,

Figur 13, Ablaufplan zur Entschlüsselung der Schlüssel für die Fernwertvorgabe

Figur 14, Ablaufplan zur Absicherung von sicherheitsrelevanten Daten in einem frei zugänglichen Speicher

Figur 15, Prüfschritt im Ablaufplan zur Absicherung von sicherheitsrelevanten Daten

Figur 16, Aufteilung der EPROM-Speicherbereiche

Figur 17, Ablaufplan zur kontinuierlichen Programmüberwachung

Die Figur 1 zeigt ein Blockschaltbild der erfindungsgemäßen Frankiermaschine mit einem Druckermodul 1 für ein vollelektronisch erzeugtes Frankierbild, mit mindestens einem mehrere Betätigungselemente aufweisenden Eingabemittel 2, einer Anzeigeeinheit 3, einem die Kommunikation mit einer Datenzentrale herstellenden MODEM 23, weitere Eingabemittel 21 bzw. Waage 22 welche über einen Ein/Ausgabe-Steuermodul 4 mit einer Steuereinrichtung 6 gekoppelt sind und mit nichtflüchtigen Speichern 5a, 5b bzw. 9, 10 und 11 für Daten bzw. Programme, welche die variablen bzw. die konstanten Teile des Frankierbildes einschließen.

Ein Charakterspeicher 9 liefert die nötigen Druckdaten für die variablen Teile des Frankierbildes zu einen flüchtigen Arbeitsspeicher 7. Die Steuereinrichtung 6 weist einen Mikroprozessor µP auf, der mit dem Ein/Ausgabe-Steuermodul 4, mit dem Charakterspeicher 9, mit dem flüchtigen Arbeitsspeicher 7 und mit nichtflüchtigen Arbeitsspeichern 5a, 5b, welche einen Kostenstellenspeicher umfassen, mit einem Programmspeicher 11, mit dem Motor einer Transport- bzw. Vorschubvorrichtung ggf. mit Streifenauslösung 12, einem Encoder (Codierscheibe) 13 sowie mit einem Uhren/Datums-Baustein 8 in Verbindung steht. Die einzelnen Speicher können in mehreren physikalisch getrennten oder in nicht gezeigter Weise in wenigen Bausteinen zusammengefaßt verwirklicht sein. Derjenige Speicherbaustein, welcher den nichtflüchtigen Arbeitsspeicher 5b umfaßt, kann beispielsweise ein EEPROM sein, der durch mindestens eine zusätzliche Maßnahme, beispielsweise Aufkleben auf der Leiterplatte, Versiegeln oder Vergießen mit Epoxidharz, gegen Entnahme gesichert wird.

In der Figur 1 ist ein Blockschaltbild einer elektronischen Frankiermaschine mit erfindungsgemäß erhöhter Sicherheit gezeigt. Die Erfindung basiert auf einer Frankiermaschine mit einem Mikroprozessor, der einen internen OTP-ROM enthält, der ein Auslesen des darin enthaltenen Programmcodes nicht erlaubt. Außerdem sind sicherheitsrelevante Daten im internen OTP-ROM gespeichert. Zur Verhinderung des Auslesens durch einen externen Eingriff können im Mikroprozessor entsprechende Sicherungsbits während der Herstellung der Frankiermaschine gesetzt werden. Dies kann ein handelsüblicher OTP-Prozessor sein, den man nach dem Programmiervorgang durch setzen/brennen einer Auslesesperre in einen solchen Zustand versetzt oder dies kann ein Mikroprozessor mit maskenprogrammierbarem ROM sein, der nach dem Herstellungsprozeß ein Auslesen des Programmcodes nicht mehr erlaubt oder nur ein Auslesen des Programmcodes und der Daten in verschlüsselter Form erlaubt.

In der Figur 2 ist ein Detail des Blockschaltbildes der elektronischen Frankiermaschine für eine Variante mit OTP in der Steuereinrichtung gezeigt. Bei dieser prinzipiellen Anordnung in der Figur 2 können Sensoren und Aktoren, wie beispielsweise die in der Figur 1 dargestellten Encoder 13 und Motor 12 wahlweise direkt oder über I/O-Ports mit dem OTP verbunden sein.

Eine bevorzugte Variante eines Mikroprozessors ist ein 8051-Prozessor mit 16kByte On-Chip-EPROM (Philips 87C51FB) Ein solcher OTP-Typ (One Time Programmable) kann nicht durch UV-Licht gelöscht werden, weil dieser kein für UV-Lichtdurchtritt geeignetes Fenster aufweist. Deshalb kann ein OTP nur einmal programmiert werden. Der interne OTP-RAM hat einen Speicherbereich von 256 Byte.

Weiter geht die Erfindung davon aus, daß der gesamte zum Betrieb einer Frankiermaschine benötigte Programmcode nicht in den mikroprozessorinternen ROM paßt, es also eines weiteren Speichers (EPROM) bedarf, der den größeren Teil des Programmcodes aufnimmt und der über den Mikroprozessorbus Programmcode dem Mikroprozessor zur Verfügung stellt. Vorteilhaft kann wird eine Anordnung angewendet werden, die den Programmspeicher in Speichersegmente aufteilt, sogenannte Speicherbänke, die es erlauben den Programmspeicherbereich über den Adressbereich des Mikroprozessor durch Benutzung von Mikroprozessor-Portleitungen beliebig zu vergrößern.

In der Figur 3 ist ein Gesamtablaufplan für eine Frankiermaschine mit erfindungsgemäß erhöhter Sicherheit gezeigt, während die Figur 4 ein erfinderisches Detail daraus, nämlich einen Ablaufplan für die Start- und Initialisierungsroutine genauer darstellt.

Aus den Figuren 3 und 4 geht hervor, daß ein Einschalten der Frankiermaschine im Schritt Start 100 erfolgt und anschließend innerhalb einer Startroutine 101 eine Funktionsprüfung mit anschließender Initialisierung vorgenommen und erst später auf eine Systemroutine 200 verzweigt wird.

BNSDOCID <EP_____0762338A2_I >

Ein Programmcode im nichtlesbaren internen OTP-ROM erlaubt nun mehrere vorteilhafte Startsicherheitsüberprüfungsroutinen aber mindestens diejenigen, wie sie in der Figur 4 benannt sind und in Verbindung mit den Figuren 7, 9 und 11 näher dargelegt werden.

Diese Routinen betreffen das Verfahren zur Absicherung von Daten und Programmcode einer elektronischen Frankiermaschine und dienen der Verbesserung der Sicherheit dieser elektronischen Frankiermaschine im Rahmen einer Startsicherheitsüberprüfung in Verbindung mit ihrer Initialisierung.

Nach dem Start erfolgt im Schritt 101 eine Startroutine und eine Initialisierung der Frankiermaschine. Solche Routinen initialisieren die Hardware und Anzeige in üblicher Weise und starten einen Timer und/bzw. Interrupt. Der Schritt 101 schließt erfindungsgemäß eine Startsicherheitsüberprüfung 1020 ein.

Eine Startsicherheitsüberprüfungsroutine, die mit ihrem Programmcode die wichtigsten extern gehaltenen Frankiermaschinen-Daten und externen Programmcode völlig gekapselt im internen ROM- und RAM- Bereich des OTP überprüft, kann, ohne daß dabei eine äußere Einwirkungsmöglichkeit in Manipulationsabsicht besteht, Manipulationen erkennen, die während des ausgeschalteten Zustandes der Frankiermaschine durchgeführt worden sind und dann den weiteren Betrieb der Frankiermaschine wirkungsvoll sperren, falls die Überprüfungsroutinen nicht fehlerfrei durchlaufen werden. In diesem Fall verbleibt der Programmablauf in einer Programmendlosschleife im OTP-ROM (error handling 1030). Erst nachdem die Checks fehlerfrei durchlaufen sind, werden die externen Speichermedien vom Mikroprozessor (Eprom lesen, RAM schreiben) benutzt und wird die Systemroutine 200 erreicht.

In der Figur 4 ist der schematische Programmablaufplan aller Funktionen, die während der Startsicherheitsüberprüfung der Frankiermaschine im OTP-ROM ausgeführt werden, dargestellt. Erfindungsgemäß umfaßt die Startsicherheitsüberprüfung der Frankiermaschine eine Vielzahl von Routinen, neben der Routine 1026 für die Absicherung des externen Programmspeichers.

Beispielsweise bezeichnet die nicht näher beschriebene Routine 1021 eine Überprüfung des internen OTP-RAM hinsichtlich seiner Betriebsfähigkeit. In den Routinen 1022 und 1023 werden die Programmversionsnummern verglichen, das heißt festgestellt, ob der gebrannte OTP mit dem EPROM einen Satz an vollständigen Programmcode bildet bzw. ob ein anderer EPROM zum OTP gehört. In der Routine 1024 wird anhand der vom Klischee-EPROM vorgegebenen Daten überprüft, ob ein gültiges bzw. zum o.g. Satz zugehöriges Klischee-EPROM im Sockel steckt. Hierbei ist als Vorteil zu erwähnen, daß das Klischee-EPROM nicht nur ausschließlich vom Servicetechniker, sondern auch problemlos von jeder anderen befugten Person in den Sockel gesteckt bzw. ausgewechselt werden darf. Spezielle Treiberschaltkreise (Buffer), welche zwischen Bus und EPROM-Sockel geschaltet ist (Fig. 2), verhindern das Auslesen von frankiermaschineninternen Daten nach außen. Andererseits können Daten jederzeit über den Sockel in die Frankiermaschine eingegeben werden.

Während die Routine 1026 die Absicherung des externen Programmspeichers und die Routine 1025 die Absicherung der von außen zugänglichen Eproms und der darin gespeicherten Daten vor Manipulationen durch Sicherheitsüberprüfung betreffen, wird in den Routinen 1027 und 1028 eine erste Überprüfung von sicherheitsrelevanten bzw. Postregisterdaten im externen NVRAM und EEPROM vorgenommen. Die Routine 1029 stellt ungültige oder reparaturfähige Datenkopien fest und beseitigt gegebenenfalls den Fehler.

Im Schritt 1029 wird - wie das in der europäischen Anmeldung EP 615 211 A1 näher erläutert wird - mindestens eine Registerprüfung der Datenstruktur der Postregister durchgeführt, um die Fehler zu protokollieren. Dort wird ein Verfahren zur Speicherkorrektur sicherheitsrelevanter Daten in einer Frankiermaschine vorgeschlagen, wobei redundant abgespeicherte Daten untereinander verglichen werden, um einen Speicherbereich mit fehlerhaften Daten wieder mit fehlerfreien Daten zu laden. Das ist aber bei einem sechsten Fehlertyp nicht mehr möglich, weil alle redundant gespeicherten Daten nun unterschiedliche Fehler haben, welche nicht mehr automatisch korrigiert werden können. Nur ein Servicetechniker könnte die Daten nach einer vorbestimmten Weise rekonstruieren, was dann nach jedem autorisiertem Öffnen vor erneuter Inbetriebnahme der Frankiermaschine zu geschehen hat. Im Schritt 1030 werden deshalb auch Maßnahmen ergriffen, um die Frankiermaschine bei Registerdatenstrukturfehlern zu sperren.

Die folgend näher beschriebene Routine 1026 für die Absicherung des externen Programmspeichers basiert auf der Speicherung eines MAC im jeweils abzusichernden Speicherbaustein. Das hat neben der erforderlichen Aufrechterhaltung der Datensicherheit vor allem den Vorteil einer Austauschbarkeit eines fehlerbehafteten Programm-EPROM's, ohne daß gleichzeitig auch der zugehörige OTP ausgetauscht werden müßte.

Zur Absicherung des externen Programmspeichers erfolgt im Schritt 1026 eine Anwendung des MAC-Verfahrens zur Überprüfung der Integrität des Programmcode externer busgekoppelter Speicher (EPROMs) vor dem Buszugriff des Prozessors und während der laufenden Programmausführung. In vorteilhafter Weise lassen sich mit einem Geheimschlüssel der unauslesbar im internen Programmspeicher versteckt ist, sichere kryptographische Funktionen realisieren, deren Sicherheit auf der Benutzung dieses Geheimschlüssels beruht. Werden Daten betreffend einer Prüfsumme (z.B. CRC) über den Speicherinhalt (Block 70) des Programmspeichers mit einer krytographischen Funktion (Block 60), wie z.B. Data-Encryption-Standard (DES), unter Verwendung dieser Geheimschlüssel (Block 61) verschlüsselt, wird eine kryptographische Prüfsumme erhalten, den sogenannten Message-Authentication-

BNSDOCID: <EP_____0762338A2_I_>

Code (MAC), der eine Prüfsumme (z.B. CRC) über den Speicherinhalt (Block 70) abbildet. Erfindungsgemäß wird dieser MAC einmal zu einem Zeitpunkt T_1 gebildet, zu dem Manipulationen ausgeschlossen sind und in einem nichtflüchtigen Speicherbereich (Block 71) des externen Programmspeichers des Mikroprozessorsystems abgespeichert. Dieser Zeitpunkt T1 wird allein beim Frankiermaschinenhersteller erreicht, wobei dieser MAC(T1), z.B. während der Programmcode-Datenerstellung im Personalcomputer, mit dem kryptographischen Prüfsummenverfahren (z.B. DES-Algorithmus) gebildet und in einem definierten Speicherbereich im Eprom-Quelldaten eingebettet wird. Die vorgenannten Daten werden beim Programmieren in den EPROM eingebrannt.

Die Figur 6 zeigt ein solches Bilden einer MAC Prüfsumme mit DES-Verfahren über externe Programm-EPROMs, wobei der MAC im Speicherbereich eingebettet wird, der dem zu schützenden Speicherbereich zugeordnet ist.

Zwar wurde bereits (ohne dies näher zu erläutern) in der EP 660269, Fig. 2a (Schritt 101) eine Startroutine und Initialisierung einer elektronischen Frankiermaschine vorgeschlagen. Weiterhin wurde eine Routine für die Initialisierung vorgeschlagen, wobei ein sicherheitsrelevanter Programmcode im OTP-abgelegt wird und wobei im OTP das Bilden einer Checksumme über den Inhalt des externen Programmspeichers und ein Vergleich erfolgt. Jedoch wurde der MAC in einem speziellen OTP mit internen NVRAM gespeichert. Außerdem wurde noch keine Maßnahmen mitgeteilt, welche verhindern, daß, sobald der Mikroprozessor mit einem ***Jump***- oder ***Callbefehl*** den internen ROM-Bereich verläßt, ein Manipulator die Kontrolle über den Mikroprozessor mit eigenem Programmcode im externen Eprom übernehmen kann und so z.B. Sicherheitsüberprüfungsroutinen, die eigentlich hinterher im OTP-ROM durchgeführt werden sollten, überspringen kann. Weiterhin wurde noch keine Maßnahmen mitgeteilt, welche verhindern, daß, sobald der Mikroprozessor den als Datenspeicher für seinen auszuführenden Programmcode dienenden externen RAM beschreibt, dieser durch einen Manipulator verändert werden kann, was den Programmablauf verändern oder stören kann.

In der Figur 7 ist ein Ablauf für das Prüfen eines externen Programm-EPROMs mit MAC-Prüfsummenverfahren auf Manipulationen dargestellt. Zur Laufzeit der Frankiermaschine kann das Mikroprozessorsystem nach dem gleichen kyptographischen (Schritt 1026.2) Prüfsummenverfahren über den zu prüfenden Speicherbereich (Schritt 1026.1) den MAC (im Schritt 1026.2) zum Zeitpunkt T_2 und später (T_{2+n}) unter Zuhilfenahme des gleichen Geheimschlüssels (Schritt 1026.3) bilden und diesen MAC (T_{2+n}) mit dem aus dem EPROM (im Schritt 1026.5) entnommenen MAC (T_1) vergleichen (siehe Schritt 1026.6). Mit einem solchen Vergleich kann auch während der Laufzeit der Frankiermaschine in einem Schritt 210 die Datenintegrität überprüft und Manipulationen der Speicherinhalte erkannt werden. Bei einem negativen Vergleich (wie Schritt 1026.7 festgestellt) können dann entsprechende Maßnahmen ergriffen werden, die einen weiteren Betrieb der Frankiermaschine verhindern (wie im Schritt 1030) oder eine Manipulation erschweren bzw. eine solche durch geeignete Maßnahmen anzeigen.

Die kontinuierliche MAC-Bildung erfolgt - wie im Schritt 210 der Fig.3 gezeigt - nach der im Schritt 101 stattfindenden Startsicherheitsüberprüfung 1020 in jedem Durchlauf der Betriebsprogrammschleife, so daß voranschreitend über jeweils eine größere Anzahl von Programmspeicherzellen mittels des kryptographischen Prüfsummenverfahrens ein relevanter MAC gebildet und mit dem jeweiligen gespeicherten, zum Zeitpunkt T1 gebildeten MAC verglichen werden kann.

Zur Erläuterung der kontinuierlichen Programmüberwachung soll auf eine - in der Figur 16 gezeigte - Aufteilung der EPROM-Speicherbereiche mit MAC-Zuordnung hingewiesen werden. Da die Überprüfung des gesamten Speicherbereiches zu lange dauern würde, ist der Speicher in Blöcke und Unterblöcke unterteilt. Zu jedem Block B gibt es einen zugehörigen MAC, der die Gültigkeit des Blocks sicherstellt. Ein Block umfaßt beispielsweise 4 KByte. Bei einem 128 KByte EPROM gibt es also 32 Blöcke und MAC-Prüfsummen. Jeder Block B ist in mehrere Subblöcke SB aufgeteilt. Diese Subblöcke SB haben eine Größe von vorzugsweise 16 Codewörtern.

Die kontinuierliche Programmüberwachung wird anhand eines in der Figur 17 gezeigten Ablaufplanes näher erläutert. Bei einem Durchlauf wird nicht über den gesamten Block ein MAC berechnet, da das zu lange dauern würde. Erfindungsgemäß wird über jeden der Subblöcke SB eines Blocks B der MAC inkrementell berechnet. Die 16 Codewörter des jeweiligen Subblocks SB werden im aktuellen Block B im Schritt 210-1 aufgerufen, um darüber insgesamt eine Prüfsumme (Checksum) und um gegebenenfalls anschließend daraus mittels DES-Verschlüsselung einen MAC zu bilden. Zu Beginn ist die Prüfsumme noch Null. Ebenfalls wird während der Startroutine der Blockzähler und der Subblockzähler auf den Stand Null gesetzt. Die Prüfsummen- bzw. die MAC-Berechnung für einen ganzen Block wird erfindungsgemäß unterbrochen und im nächsten Durchlauf weitergeführt. Beispielsweise wird die Prüfsumme bei jedem Durchlauf kumuliert und dann gegebenenfalls der MAC gebildet. Der Subblockzählerstand SBZ wird im Schritt 210-2 inkrementiert, um fortschreitend im nächsten Durchlauf wieder im Schritt 210-1 kumulieren zu können und um dann den jeweiligen inkrementellen MAC zu bilden. Nach dem Schritt 210-2 zum Inkrementieren des Subblockzählers wird über einen Prüfschritt 210-3 zum Punkt e der Systemroutine verzweigt, wenn der maximale Subblockzählerstand SBZmax noch nicht erreicht ist. Anderenfalls sind alle Subblocke eines Blockes durchlaufen worden und der Endstand bei der Prüfsummenbildung bzw. bei der MAC-Bildung ist erreicht. Nun kann in einem weiterem Schritt 210-4 die vorgenannte kumulierte Prüfsumme

BNSDOCID <EP_____0762338A2 I_>

bzw. der MAC mit einem zugehörig gespeicherten Wert verglichen werden. Der zugehörig gespeicherte Wert ist eine Prüfsumme bzw. ein MAC, welcher den Subblock authentifiziert. Der zugehörig gespeicherte Wert kann im selben zu prüfenden EPROM oder in einem andern Speicher, beispielsweise im internen OTP-ROM, zum Zeitpunkt T1, vorzugsweise beim Frankiermaschinenhersteller bei der Programmierung des OTP, eingespeichert worden sein.

Wird im nachfolgenden Schritt 210-5 festgestellt, daß keine Identität und somit ein Fehler vorliegt, wird auf eine - nicht gezeigte Fehlerroutine verzweigt. Beispielsweise wird ein Flag gesetzt, welches in Schritt 409 des Frankiermodus 400 ausgewertet wird (Fig.5). Anderenfalls, bei Identität, ist die Autentifizierung erfolgreich abgeschlossen worden und und es werden der Schritt 210-6 zur Blockinkrementation und der Schritt 210-7 zur Rücksetzung des Subblockzählerstandes und der Prüfsumme auf den Wert Null erreicht.

Der jeweils aktuelle Block B wird durch den Blockzählerstand BZ eines Blockzählers ermittelt, welcher hard- oder softwaremäßig realisiert werden kann. Ebenso wird der jeweils aktuelle Subblock SB durch den Subblockzählerstand SBZ eines Blockzählers ermittelt, welcher ebenfalls hard- oder softwaremäßig realisiert werden kann. Anschließend wird der nächste Subblock

Bei jedem Durchlauf wird über die 16 Codewörter eines Subblockes eine inkrementelle Prüfsumme gebildet. Beim Erreichen des jeweiligen Blockendes (im vorgenannten Fall nach 4096/16 = 256 Durchläufen durch die Systemroutine) wird die kumulierte Prüfsumme mit dem zugehörigen Wert bzw. die MAC's verglichen. Bei Übereinstimmung wird wieder der Blockzähler im Schritt 210-6 auf den folgenden Block (BZ := BZ+1) gesetzt und der Subblockzähler auf den Anfang des neuen Blocks gesetzt (SBZ := 0). Die Prüfsumme ist somit ebenfalls wieder Null. Anschließend wird im Schritt 210-8 geprüft, ob alle Blöcke abgearbeitetet wurden. Wurde der letzte Block abgearbeitet, so wird der Blockzähler wieder auf den ersten Block gesetzt (BZ := 0) und dann auf den Punkt e verzweigt. Somit wird das System kontinuierlich überprüft.

Das vorgeschlagene Ausführungsbeispiel ist an jedes System anpaßbar. Abhängig vom verwendeten System kann es sinvoll sein, die Blockgröße und die Subblockgröße anders zu wählen. Eine zu geringe Blockgröße hat aber den Nachteil, daß die Anzahl der MAC-Prüfsummen steigt und damit auch mehr Speicherplatz verbraucht wird. Eine zu geringe Subblockgröße bedeutet, daß sehr häufig Prüfsummen berechnet werden und Abfragen erfolgen, so daß der Zeitbedarf wieder steigt.

Durch die voranschreitend über jeweils eine größere Anzahl von Programmspeicherzellen erfolgende Prüfung wird erreicht, daß die Zeit bis zu einem MAC-Prüfsummenvergleich über den gesamten Speicherinhalt relativ kurz ausfällt. Das Intervall zwischen den Prüfsummenvergleichen kann außerden noch mit - einer nicht gezeigten - zeitlichen Überwachung verknüpft werden, so daß ein Anhalten des Programms erkannt wird und zur gleichen Fehlerbehandlung, wie bei einem negativen MAC-Vergleich führt.

Die Figur 8 zeigt das Bilden einer MAC-Prüfsümme mit DES-Verfahren über EPROMs im Sockel der offenen Postklappe. Dies ist eine weitere vorteilhafte Anwendung des MAC-Verfahrens zur Überprüfung der Integrität der Daten und des Programmcodes von Eproms, die bei einer Frankiermaschine mit geöffneter Postklappe in den extern zugänglichen Sockel eingesetzt werden.

In EP 660 269 wird noch von einer Frankiermaschine ausgegangen, die eine verschließbare und versiegelte Klappe hat, die den Zugriff auf die dahinter liegende Hardware (EPROM-Sockel) nur einem begrenztem speziell vertrauenswürdigen Personenkreis erlaubt. Hier konnte davon ausgegangen werden, daß durch diese Personen kein Manipulation der Frankiermaschine erfolgt. Es wurde nun eine Lösung gefunden, daß die Sicherheit für eine Frankiermaschine aufrecht erhalten werden kann, die eine teilweise geöffnete Postklappe aufweist. Das hat den Vorteil, daß der Anwender Zugriff auf den Klischee-EPROM-Sockel hat und den Klischee-EPROM selbständig wechseln kann. Dieser Sockel ist, wie in Figur 2 zu entnehmen, mit dem Mikroprozessorbus verbunden, d.h. eine Manipulation könnte so erfolgen, daß ein Manipulator ein manipuliertes Programm-EPROM einsetzt, das wie ein RESET-Eprom die Kontrolle über das Mikroprozessorsystem übernimmt und somit Geldwerte, Einträge oder Sicherheitseinträge in der Frankiermaschine gezielt verändert oder daß er ein manipuliertes Klischee-Eprom einsetzt, daß veränderte Druckdaten des Wertstempels enthält (Ort des Absenders, Postleitzahl des Absenders) und eine Manipulation des Wertstempelabdruckes zur Folge hätte.

Die Figur 8 zeigt die Absicherung eines weiteren externen EPROM's. Auch hier läßt sich das bereits oben erwähnte Prinzip der MAC-Absicherung über die Speicherbereiche anwenden, da mit einem Geheimschlüssel der unauslesbar im internen Programmspeicher (OTP-ROM) versteckt ist, sich sichere kryptographische Funktionen realisieren lassen, deren Sicherheit auf der Benutzung dieses Geheimschlüssels beruht. Verschlüsselt man eine Prüfsumme dieser Datenbereiche (Block 40) mit einer krytographischen Funktion (Block 60) z.B. DES unter Verwendung dieser Geheimschlüssel (Block 40) entsteht eine krytographische Prüfsumme, welche den Speicherinhalt abbildet. Dieser MAC muß einmal zu einem Zeitpunkt T_1 gebildet werden, zu dem Manipulationen ausgeschlossen sind und wird in dem betreffenden Eprom, der in dem Klischeesockel eingesetzt wird (Klischeeeprom, RESET-Eprom), abgespeichert (Block 41). Dieser MAC(T_1) wird z.B. während der Programmcode-Datenerstellung des RESET-Eproms im Personalcomputer und bei der Klischeedatenerstellung mit dem kryptographischen Prüfsummenverfahren (z.B. DES-Algorithmus) gebildet und in einem definierten Speicherbereich in den Eprom-

BNSDOCID: <EP_____0762338A2_I_>

Quelldaten eingebettet.

Die Figur 9 zeigt das Prüfen eines EPROMs im Klischeesockel mit MAC-Prüfsummenverfahren auf Manipulation. Zur Laufzeit der Frankiermaschine kann das Mikroprozessorsystem nach dem gleichen kryptographischen Prüfsummenverfahren (Schritt 1025.2) über den zu prüfenden Speicherbereich (Schritt 1025.1) den MAC zu den Zeitpunkt T_2 der Startsicherheitsüberprüfung unter Zuhilfenahme (Schritt 1025.3) des gleichen Geheimschlüssels bilden und diesen MAC (T_2) mit dem EPROM entnommenen (Schritt 1025.5) MAC (T_1) vergleichen (Schritt 1025.6). Durch diesen Vergleich (Schritt 1025.6) lassen sich die Datenintegrität der Wertstempeldaten überprüfen und eine Manipulationen des Programmcodes erkennen (Schritt 1025.7). Bei einem negativen Vergleich können dann entsprechende Maßnahmen ergriffen werden, die einen weiteren Betrieb der Frankiermaschine verhindern (error handling 1030).

Die Figur 11 betrifft das Prüfen ausgewählter Postdatenwerte in einer elektronischen Frankiermaschine, die mit einem MAC abgesichert sind. Eine solche Prüfung wird beispielsweise im Schritt 1027 während der Start- und Initialisierungsroutine, im Kommunikationsmodus 300 und im Frankiermodus 400 durchgeführt.

Die Startsicherheitsüberprüfung in der Start- und Initialisierungsroutine wird also mittels eines ausgewählten Prüfsummenverfahren innerhalb eines OTP-Prozessors (ONE TIME PROGRAMMABLE) durchgeführt, der intern die entsprechenden Programmteile und außerdem den Code zur Bildung eines MAC (MESSAGE AUTHENTIFICATION CODE) gespeichert enthält, weshalb der Manipulator die Art des Prüfsummenverfahrens nicht nachvollziehen kann. Auch weitere sicherheitsrelevante Schlüsseldaten und Abläufe sind ausschließlich im Inneren des OTP-Prozessors gespeichert, um eine MAC-Absicherung über die Postregister zu legen.

In der EP 660 269 ist die Absicherung der Registerwerte R1,R2,R3, die in einem nichtflüchtigen NVRAM gespeichert sind (siehe Figur 1), mit einem MAC bereits ausgeführt. Die folgende Ausführung erweitert diese Registerabsicherung, um gezielt eine noch höhere Sicherheit der Frankiermaschine zu erreichen. Es sollen zusätzlich weitere Fälle abgesichert werden:

1. Stückzählerregister R4, mit dem in der Frankiermaschine folgende sicherheits-
relevante Überprüfungen durchgeführt werden:

- Suspicious Mode
- Abdruck des R4-Wertes im Frankierstempelbild zur visuellen Postkontrolle
- Sleeping Mode

Eine Manipulation von R4 würde diese aufgelisteten Sicherheitsüberprüfungen in Frage stellen und deshalb wird R4 in die nachfolgende MAC-Absicherung von Registern einbezogen.

2. Seriennummer, mit der das Benutzen von NVRAM's aus anderen Frankiermaschinen verhindert werden kann.
Der Vorschlag geht von einer Frankiermaschine aus, die die Registerdaten, die Seriennummer und andere zur Laufzeit der Frankiermaschine veränderliche Sicherheitsrelevante Daten (z.B Codewort Y, Flags) in einem NVRAM hält (siehe Figur 1) der nicht auf der Steuereinheit aufgelötet ist, sondern in einem handelsüblichen Sockel steckt, damit im Servicefall dieser NVRAM gezogen und mit einem speziellen Servicecomputer ausgelesen werden kann um z.B. Registerdaten zu auszulesen.

Ein Manipulator könnte die Frankiermaschine öffnen und sich von diesem NVRAM oder dem einer anderen Frankiermaschine, die einen konsistenten Datensatz (Geldwerte, Registerstände, MACs, Sicherheitsdaten, FLAGs) beinhaltet, Kopien erzeugen. Nun führt er gezielt Manipulationen am Datensatz durch, indem er z.B den abgerechneten Frankierwert verringert. Bei einer Inspektion oder der nächsten Fernwertvorgabe würde diese Manipulation auffallen z.B. durch die Überprüfungen des Suspicous Mode.

Bezieht man die Seriennummer, die eine eindeutige Kennzeichnung einer einzelnen Frankiermaschine ist, also auch die eindeutige Kennzeichnung des Datensatzes der Frankiermaschine ist, mit in die MAC-Absicherung von Registerdaten ein, so läßt sich ein Datensatz im NVRAM aus einer anderen Frankiermaschine nicht benutzen, weil die Seriennummer noch in einem anderen nichtflüchtigen Speicher (z.B. EEPROM) eingespeichert ist, der nicht aus der Frankiermaschine heraus genommen werden kann.

Bei einem Vergleich der verschieden abgespeicherten Seriennummern würde die Manipulation erkannt werden und die Frankiermaschine blockieren.
Um diese erhöhte Sicherheit zu erreichen, werden folgende Register mit einem MAC abgesichert und sind somit gegenüber Manipulationen abgesichert:

- Restsummenregister R1
- Vorgabesummenregister R3
- Stückzahlregister R4
- Maschinennummer Nr.

Das Prinzip dieser MAC-Generierung ist in Figur 10 dargestellt. Nach jeder Änderung der Register z.B. Frankieren wird der MAC neu berechnet, in dem die Register mit der kryptographischen Funktion (Block 60), Data-Encryption-Standard (**DES**), unter Verwendung (Block 63) des Geheimschlüssels K_{reg} verschlüsselt werden. Das Ergebnis der Verschlüsselung, der **MAC**, wird in der dafür reservierten Datenbereich 50a im NVRAM gespeichert.
Der Register-MAC wird wie die anderen Postregister

BNSDOCID <EP_____0762338A2_I_>

mehrfach im NVRAM abspeichert und zu bestimmten Ereignissen in dem EEPROM abgespeichert, da dieser nur eine begrenzte Anzahl von Speicherzyklen zuläßt.
Die Figur 11 zeigt den prinzipiellen Ablauf einer Überprüfung bei eingeschalteter Frankiermaschine. Zur Laufzeit der Frankiermaschine kann das Mikroprozessorsystem nach dem gleichen kryptographischen Prüfsummenverfahren (Schritt 1027.2) über den zu prüfenden Speicherbereich 50a (Schritt 1027.1) den MAC (Schritt 1027.4) zu den Zeitpunkten Startsicherheitsüberprüfung 1020, vor jeder Frankierung (Frankiermodus 400) und vor jeder Fernwertvorgabe (Kommunikationsmodus 300) unter Zuhilfenahme des gleichen Geheimschlüssels (Block 63, (Schritt 1027.3) bilden und diese generierten MAC's (Schritt 1027.4) mit dem entnommenen (Schritt 1027.5) MAC (T1) vergleichen im Schritt 1027.6).
Bei einem negativen Vergleich (Schritt 1027.7) können dann entsprechende Maßnahmen (Schritt 1030) ergriffen werden, die einen weiteren Betrieb der Frankiermaschine verhindern.

Die Figur 5 zeigt den Ablaufplan für einen Frankiermodus mit erfindungsgemäß integrierten Prüfschritten, die vor dem Drucken ausgeführt werden. Diese umfassen ebenfalls die in den Figuren 10 und 11 näher erläuterte Absicherung ausgewählter Postdatenwerte in einer elektronischen Frankiermaschine mit einem MAC.

Die Erläuterung der Abläufe nach dem - in der Figur 5 gezeigten - Frankiermodus erfolgt in Verbindung mit dem - in den Figuren 1, 2 bzw. 3, 4 dargestellten - Blockschaltbildern bzw. Abläufen.

Die Erfindung geht davon aus, daß nach dem Einschalten automatisch der Postwert im Wertabdruck entsprechend der letzten Eingabe vor dem Ausschalten der Frankiermaschine und das Datum im Tagesstempel entsprechend dem aktuellem Datum vorgegeben werden, daß für den Abdruck die variablen Daten in die festen Daten für den Rahmen und für alle unverändert bleibenden zugehörigen Daten elektronisch eingebettet werden. Diese variablen Daten der Fensterinhalte werden nachfolgend kurz als Fensterdaten und alle festen Daten für den Wertstempel, den Tagesstempel und den Werbeklischeestempel als Rahmendaten bezeichnet. Die Rahmendaten sind einem ersten Speicherbereich eines Nurlesespeichers (ROM), welcher zugleich als Programmspeicher 11 dient, entnehmbar. Die Fensterdaten werden einem zweiten Speicherbereich entnommen und entsprechend der Eingabe in Speicherbereichen B_j des nichtflüchtigen Arbeitsspeichers 5 gespeichert. Für eine solche Klischee- und oder Frankierbildverarbeitung ist ein - in der Fig. 4 gezeigter - Schritt 1040 vorgesehen. Dieser Schritt umfaßt eine automatische Routine für den Aufruf von Bildpunktdateien, die Zuordnung und Einbettung von Pixelbilddaten der festen und semivariablen sowie variablen Druckbilddaten. Das zugehörige Programm ist im Programm-EPROM und/oder im internen OTP-ROM gespeichert. Da bis zum Schritt 1040 keine Programmverzweigung auf im externen Programm-EPROM gespeicherte Programmteile erfolgt, kann keine Manipulation der Druckbilderstellung erfolgen.
Sie sind den vorgenannten Speichern natürlich auch jederzeit während der Laufzeit der Frankiermaschine zwecks eines neuen Zusammensetzens zu einer Gesamtdarstellung eines Frankierbildes entnehmbar. Dabei ist in einer bevorzugten Variante vorgesehen, die hexadezimalen Fensterdaten in lauflängencodierter Form in die jeweils getrennten Speicherbereiche B_1 bis B_4 des nichtflüchtigen Arbeitsspeichers 5a zu übertragen und dort abzuspeichern. Außerdem läuft die Zeit im Uhren/ Datums-Baustein 8 ständig auch bei ausgeschalteter Frankiermaschine weiter. Wird also der Schritt 401 im Frankiermodus 400 erreicht, wurde ggf. auch ohne manuelle bzw. erneute externe Daten-Eingabe nach dem Einschalten der Frankiermaschine auf bereits gespeicherte Daten zurückgegriffen werden. Diese Einstellung betrifft insbesondere die letzte Einstellung der Frankiermaschine hinsichtlich des Portowertes, welche im Schritt 209 angezeigt wird, bevor die Druckdatenaufbereitung erfolgt. Hierbei werden die aktuellen variablen Pixelbilddaten (Datum und Portowert) in die festen Rahmenpixelbilddaten eingebettet. Anschließend erfolgt im Schritt 301 des Kommunikationsmodus 300 bzw. in weiteren Schritten, wie beispielsweise im Schritt 401 des Frankiermodus 400 eine Abfrage der Eingabemittel auf eventuelle weitere Eingaben.

Im Schritt 209 werden die Daten aus den vorgenannten Speicherbereichen entsprechend einer vorbestimmten Zuordnung zu einem Pixeldruckbild noch vor dem Druck zusammengesetzt. Die variable Information im dafür vorgesehenen Fenster können nachträglich ergänzt und modifiziert werden. Um Zeit einzusparen, werden nur die Teile einer graphischen Darstellung bei einer Änderung neu im nichtflüchtigen Arbeitsspeicher eingespeichert, die tatsächlich geändert werden. Im Programmspeicher 11 liegt ein erster Speicherbereich A (u.a. für die Daten der konstanten Teile des Frankierbildes) und im Klischee-EPROM liegt ein weiterer Speicherbereich A_{Ai} (für den Werbeklischeerahmen) vor. Die Subspeicherbereiche A_i, A_{Ai} sind für i = 1 bis m Rahmen- oder Fixdaten vorgesehen, wobei ein zugeordneter Index i den jeweiligen Rahmen kennzeichnet, welcher vorzugsweise einer bestimmten Kostenstelle zugeordnet ist. Die entsprechende Zuordnung der jeweiligen Kostenstelle zu den Rahmendaten wird nach dem Einschalten automatisch abgefragt. In einer in der EP 658 861 A1 vorgeschlagenen Variante kann nach jeder Auswahl eines anwenderspezifischen Klischees durch Eingabe einer Klischee-Nummer die Kostenstelle automatisch zugeordnet und in den Speicherbereich C eingegeben werden. In einer anderen - nicht gezeigten - Variante muß nach jedem Einschalten während der Startroutine die Kostenstelle erneut in den Speicherbereich C eingegeben werden.

Im Charakterspeicher 9 sind alle alphanumerischen Zeichen bzw. Symbole pixelweise als binäre Daten abgelegt. Die Daten für alphanumerische Zeichen bzw.

BNSDOCID: <EP_____0762338A2_I_>

Symbole werden im nichtflüchtigen Arbeitsspeicher 5 komprimiert in Form von Hexadezimalzahlen abgespeichert. Sobald die Nummer der Kostenstelle eingegeben im Speicherbereich C gespeichert vorliegt, werden die komprimierten Daten aus dem Programmspeicher 11 mit Hilfe des Charakterspeichers 9 in ein binäre Pixeldaten aufweisendes Druckbild umgewandelt, welches in dekomprimierten Form im flüchtigen Arbeitsspeicher 7 gespeichert wird. Zur Erläuterung der Erfindung werden nachfolgend Arbeitsspeicher 7a, 7b und Pixelspeicher 7c verwendet, obwohl es sich hierbei physikalisch vorzugsweise um einen einzigen Speicher handelt. Aus Sicherheitsüberlegungen heraus, werden die wesentlichen Bilderzeugungsprogrammschritte im internen OTP-RAM ablaufen und sind somit nicht manipulierbar.

Die Speicherbereiche im nichtflüchtigen Arbeitsspeicher 5 können eine Vielzahl von Subspeicherbereichen enthalten, unter welchen die jeweiligen Daten in Datensätze gespeichert vorliegen. Die Subspeicherbereiche B_j sind für j = 1 bis n Fensterdaten vorgesehen, wobei verschiedene Zuordnungen zwischen den Subspeicherbereichen der verschiedenen Speicherbereiche vorbestimmt gespeichert sind.

In einem jeden Datensatz eines Subspeicherbereiches A_i A_{Ai}, B_j sind abwechselnd nacheinander Steuercode und lauflängencodierte Rahmen- bzw. Fensterdaten enthalten. Vor dem Druck werden im Schritt 209 aus dem nichtflüchtigen Programmspeicher (PSP) 11 die jeweiligen ausgewählten festen Daten in erste Register 701, 711, 721,..., des flüchtigen Arbeitsspeichers 7a übernommen, wobei während der Übernahme Steuercodes dekodiert und in einem gesonderten Speicherbereich des Arbeitsspeichers 7b gespeichert werden. Ebenso werden die jeweiligen ausgewählten Fensterdaten für den Poststempel und den Portostempel in zweite Register 702, 712, 722,..., geladen. Vorzugsweise werden die Register von Subspeicherbereichen im Speicherbereich des Arbeitsspeichers 7a gebildet. In der bevorzugten Variante sind diese vorgenannten Register Bestandteil der Mikroprozessorsteuerung 6. Durch Dekomprimieren werden die lauflängencodierten hexadezimalen Daten in entsprechende binäre Pixeldaten überführt.

Die Erfindung besteht weiterhin in einer Durchführung von Authentizitätsprüfungen im Ergebnis der Druckdateneingabe im Schritt 1040 für Rahmen und/oder Fensterdaten während der Start- und Initialisierungsroutine 101 und im Schritt 209 für sicherheitsrelevante Fensterdaten, welche bei der Druckdateneingabe geändert wurden, wobei bei fehlender Authentizität Schritte zum Verhindern einer weiteren Programmausführung bzw. einer vom OTP-Prozessor nach extern führenden Programmverzweigung im Rahmen vorgenannter Systemroutine (200) und wobei bei bestehender Authentizität Schritte zur weiteren Programmausführung im Rahmen vorgenannter Systemroutine (200) durchgeführt werden.

Die Figur 14 zeigt einen Ablaufplan zur Absicherung von sicherheitsrelevanten Daten in einem frei zugänglichen Speicher bei einer elektronischen Frankiermaschine. Im Schritt 209-1 erfolgt eine Eingabe zur Veränderung von Fensterdaten. Die Eingabe wird im Schritt 209-2 angezeigt und dann auf einen ersten Prüfschritt 209-3 aus einer Anzahl Prüfschritten 209-3 bis 209-12 verzweigt. Im externen Programmspeicher (EPROM) befinden sich beispielsweise auch Druckdaten des Wertstempels und andere Daten, wie beispielsweise Ort des Absenders, Postleitzahl des Absenders usw., die durch das anhand der Figur 14 erläuterten Verfahren vor Manipulation geschützt werden sollen. Die Prüfschritte erlauben eine Verzweigung auf jeweils einen der Schritte 209-4 bis 209-11, falls bei der Eingabe ein anderer Wert, Slogan, Klischee oder andere Daten ausgewählt wurden. Damit hat das beschriebene Verfahren eine ausreichende Sicherheit, obwohl der MAC jeweils nur über den Teilbereich im EPROM gebildet ist, der Daten entsprechend der Auswahl enthält. Anschließend wird über einen Schritt 209-20 zur Rücksetzung des Schleifenzählers auf den Schritt 209-1 zurückverzweigt. Sind alle Prüfschritte 209-3 bis 209-12 ohne Änderung bzw. Auswahl eines neuen Wertes bzw. Daten durchlaufen worden, dann wird der Punkt e erreicht.

Das in EP 0 660 269 A2 mitgeteilte Verfahren, in welchem die Überprüfung des Programmes mittels MAC nur einmal zu Beginn der Laufzeit der Frankiermaschine erfolgt, wird erfindungsgemäß durch zusätzliche Sicherheitsüberprüfungen der einzelnen nachträglich geänderten Fensterdaten verbessert. In vorteilhafter Weise kann nun ein nachträgliches Austauschen der EPROM-Daten während der Laufzeit der in Betrieb befindlichen Frankiermaschine erkannt werden. Eine Manipulation oder Unterschieben von manipulierten Daten in dem Moment, wo die Daten eingelesen werden sollen, wird damit unmöglich gemacht.

In der Figur 15 sind die Schritte 209-10 bzw. 209-11 näher erläutert. Wird keine Neueingabe erkannt (Schritt 2090) wird zum Schritt 209-20 zurückverzweigt. Vor der Anwendung des MAC werden die abzusichernden externen EPROM-Daten vollständig in den Speicher der Frankiermaschine geladen (Schritt 2091) und über diesen RAM-Bereich wird danach ein MAC gebildet (Schritt 2092). Dieser MAC wird im Schritt 2094 mit einem vorberechneten MAC (Schritt 2093) verglichen, der an geeigneter Stelle abgelegt ist, vorzugsweise im externen EPROM. Der Vorteil dieser Variante liegt nun darin, daß jeweils nur solche Daten in der Frankiermaschine verwendet werden, die die Sicherheitsprüfung bestanden haben, da das von außen zugängliche EPROM und somit die Daten für die Prüfung und die Weiterverarbeitung hierbei nur einmal gelesen werden. Diese Vorgehensweise verhindert, daß die Daten nachträglich manipuliert werden können (z. B. durch Umschalten des externen EPROMs), da zum Bilden des MAC und zur Weiterverarbeitung der Daten diese nur **einmal** gelesen werden.

Fällt der Vergleich von gebildetem MAC und dem Referez-MAC, der sich vorzugsweise im externen ROM

BNSDOCID <EP_____0762338A2_I_>

befindet, negativ aus, so können geeignete Maßnahmen erfolgen. Vorzugsweise wird zwecks Fehlerauswertung und Anzeige über den Schritt 209-13 auf den Schritt 209-14 verzweigt.

Im externen EPROM lassen sich die externen Daten in Speicherbereichen unterteilt nach Datensätzen abspeichern, die jeweils nicht gleichzeitig in der Frankiermaschine benötigt werden. Dieses Verfahren erlaubt eine **Zeitersparnis** beim Prüfen der externen Daten, weil hier nur über einen **Teilbereich** ein MAC gebildet und mit dem im EPROM gespeicherten verglichen werden muß. Der für die Prüfung des MAC in der Frankiermaschine benötigte Speicher wird dadurch verringert. Existieren z. B. fünf externe Datenbereiche (Werbeklischees, Wahldrucke, o. a.), so braucht beispielsweise nur 1/5 der Gesamtdatenmenge in den internen Speicher übertragen werden (geringerer Speicherbedarf) und auch für das Bilden des MAC wird nur ca. 1/5 der Zeit benötigt. Über alle vier nicht benötigten Datenbereiche braucht also keine Prüfung zu erfolgen. Je nach Anzahl der abzusichernden Datenbereiche befindet sich die gleiche Anzahl an Referenz-MACs auch im externen Speicher (EPROM bzw. ROM).

In anderen Varianten können sich die MACs auch im NV-RAM der Frankiermaschine oder sogar im internen ROM der Frankiermaschine befinden. Werden die MACs im internen NV-RAM abgelegt, so hat dies auch den Vorteil, daß man auch ein nicht abgesichertes externes EPROM bzw. ROM durch Eingabe eines Codes in die Frankiermaschine authorisiert. Dadurch brauchen bei der Erzeugung der externen ROMs keine festen Schlüssel eingesetzt zu werden, jede Frankiermaschine kann über einen eigenen Schlüssel für das Erzeugen der MACs verfügen.

Die Sicherheit dieses neuen Verfahrens beruht nun darauf, daß sich im internen OTP-ROM der Frankiermaschine ein oder mehrere unzugängliche Verfahren (z. B. DES) und/oder ein oder mehrere unzugängliche Schlüssel befinden, die für das Bilden des MAC herangezogen werden. Die selben Schlüssel bzw. die selben Verfahren sind auch für die im ROM gespeicherten MACs bei der Erstellung des ROMs verwendet worden.

Bei der Verwendung dieses Verfahrens für die Absicherung von komprimierten Klischeedaten wird der MAC über die entpackten Daten im RAM gebildet. Dadurch erreicht man eine zusätzliche Speicherplatzersparnis, da komprimierte und entkomprimierte Daten nicht gleichzeitig im Speicher der Frankiermaschine abgelegt werden müssen.

In einer anderen Variante können die externen Daten auch unkomprimiert vorliegen, wobei die Daten dann in den internen Speicher direkt übernommen werden und dann über den internen Speicher oder Teile davon der MAC gebildet wird. Die separate Absicherung der einzelnen Klischeeteile hat darüberhinaus den Vorteil, daß der Zeitbedarf für das Prüfen des MAC beim Anwählen eines Klischees gering bleibt, da immer nur die Klischeeteile geprüft werden, die gerade benötigt werden. Für die Prüfung der Daten in einem Klischeespeicher (z. B. ROM) ist daher nicht nur ein MAC vorgesehen, sondern jedes Einzelklischee (Werbeklischee, Wahldrucke bzw. Slogan oder andere Teile, wie beispielsweise die "Entgelt bezahlt"- Leiste) besitzt einen eigenen MAC.

Neben Klischeedaten lassen sich auch andere in die Frankiermaschine einzubringende Daten durch dieses Verfahren absichern. Diese Daten können sich dabei in einem externen ROM, in einem externen RAM, in einem externen NV-RAM, auch auf einer Chipkarte oder auch in einer Kombination der vorgenannten befinden. Die Prüfung erfolgt dabei wiederum erst nach der Übertragung der Daten in den internen Speicher der Frankiermaschine.

Werden im Schritt 209-11 festgestellt, daß die MACs nicht identisch sind so kann wie im vorliegenden Fall im Schritt 209-14 der Fehler zur Anzeige gebracht werden und die Maschine daraufhin blockieren. Eine andere Möglichkeit, z. B. beim Absichern von Klischeedaten besteht darin, ein Standardklischee für diesen Fall zu drucken, welches auf eine Manipulation hinweist. Dabei kann dieses Klischee an Stelle des manipulierten Klischees oder zusätzlich gedruckt werden. Es ist auch möglich, ein anderes Klischee (z.B. Datum, Wert) so zu verändern, daß eine Manipulation erkennbar ist.

Die einmal aufgerufenen konstanten Teile des Frankierbildes stehen im Pixelspeicherbereich I im flüchtigen Pixelspeicher 7c ständig dekodiert zur Verfügung. Für eine schnelle Änderung der Fensterdaten, existiert ein zweiter Speicherbereich B im nichtflüchtigen Arbeitsspeicher 5.

Die Zahlenketten (sTrings), die für die Erzeugung der Eingabedaten mit einer Tastatur 2 oder aber über eine an die Ein/Ausgabeeinrichtung 4 angeschlossene, den Portowert errechnende, elektronische Waage 22 eingegeben werden, werden automatisch im Speicherbereich D des nichtflüchtigen Arbeitsspeichers 5 gespeichert. Außerdem bleiben auch Datensätze der Subspeicherbereiche, zum Beispiel B_j, C usw., erhalten. Damit ist gesichert, daß die letzten Eingabegrößen auch beim Ausschalten der Frankiermaschine erhalten bleiben, so daß nach dem Einschalten automatisch der Portowert im Wertabdruck entsprechend der letzten Eingabe vor dem Ausschalten der Frankiermaschine und das Datum im Tagesstempel entsprechend dem aktuellem Datum vorgegeben wird. Ist eine Waage 22 angeschlossen, wird der Portowert aus dem Speicherbereich D entnommen. Im Schritt 401 wird geprüft, ob eine Eingabe vorliegt. Bei einer erneuten Eingabeanforderung im Schritt 401 wird auf den Schritt 209 zurückverzweigt.

Anderenfalls wird über die Schritte 402 und 404 zur Erhöhung eines Durchlaufzählers und zur Prüfung der Anzahl an Durchläufen auf den Schritt 405 verzweigt, um die Druckausgabeanforderung abzuwarten. Durch einen Briefsensor wird der zu frankierende Brief detektiert und damit eine Druckanforderung ausgelöst. Somit kann auf die Abrechnungs- und Druckroutine im Schritt

BNSDOCID: <EP_____0762338A2_I_>

406 verzweigt werden. Liegt keine Druckausgabeanforderung (Schritt 405) vor, wird zum Schritt 209 (Punkt t) zurückverzweigt.

Wenn nach der - in der Figur 5 dargestellten - bevorzugten Variante nunmehr zum Punkt t zurückverzweigt und der Schritt 301 erreicht wird kann jederzeit ein Kommunikationsersuchen gestellt oder eine andere Eingabe gemäß den Schritten zum Datenwechsel 209, Testanforderung 212, Registerprüfung 214 sowie Eingabeanforderung 401 getätigt werden. Es werden wieder Schritte 401 bis 404, wie bei der Variante nach Figur 5 gezeigt, durchlaufen. Bei einer vorbestimmten Anzahl an Durchläufen wird vom Schritt 404 auf den Schritt 408 verzweigt. Das alternatives Abfragekriterium kann im Schritt 404 abgefragt werden, um im Schritt 408 ein Standby-Flag zu setzen, wenn nach einer vorbestimmten Zeit noch keine Druckausgabeanforderung vorliegt. Wie bereits oben erläutert, kann das Standby-Flag im auf den Kommunikationsmodus 300 folgenden Schritt 211 abgefragt werden. Damit wird nicht auf den Frankiermodus 400 verzweigt, bevor nicht die Checksummenprüfung die Vollzähligkeit aller oder mindestens ausgewählter Programme ergeben hat.

Falls eine Druckausgabeanforderung im Schritt 405 erkannt wird, werden weitere Abfragen in den nachfolgenden Schritten 409 und 410 sowie im Schritt 406 getätigt. Beispielsweise werden im Schritt 409 das Vorhandensein authentischer Registerwerte (Fig. 11) und im Schritt 410 das Erreichen eines weiteren Stückzahlkriterium und im Schritt 406 die in bekannten Weise zur Abrechnung eingezogenen Registerdaten abgefragt. Außerdem wird, wie bereits anhand der Figur 10 erläutert, eine Absicherung ausgewählter Register im NVRAM der Frankiermaschine durch MAC-Bildung durchgeführt. War die zum Frankieren vorbestimmte Stückzahl bei der vorhergehenden Frankierung verbraucht, d.h. Stückzahl gleich Null, wird vom Schritt 410 automatisch zum Punkt e verzweigt, um in den Kommunikationsmodus 300 einzutreten, damit von der Datenzentrale eine neue vorbestimmte Stückzahl S wieder kreditiert wird. War jedoch die vorbestimmte Stückzahl noch nicht verbraucht, wird vom Schritt 410 auf die Abrechnungs- und Druckroutine im Schritt 406 verzweigt. Ein spezieller Sleeping-Mode-Zähler wird im Schritt 406, d.h. während der unmittelbar vor dem Druck erfolgenden Abrechnungsroutine veranlaßt, einen Zählschritt weiterzuzählen. Ebenso die Anzahl von gedruckten Briefen, und die aktuellen Werte in den Postregistern werden entsprechend der eingegebenen Kostenstelle in nichtflüchtigen Speichern 5a, 5b der Frankiermaschine in der Abrechnungsroutine 406 registriert und stehen für eine spätere Auswertung zur Verfügung.

Die Registerwerte können bei Bedarf im Anzeigemodus 215 abgefragt werden. Es ist ebenfalls vorgesehen, die Registerwerte oder andere Servicedaten mit dem Druckkopf der Frankiermaschine zu Abrechnungs- oder Kontrollzwecken auszudrucken. Das kann beispielsweise ebenso erfolgen, wie das normale Drucken des Frankierbildes wobei jedoch anfangs ein anderer Rahmen für fixe Bilddaten gewählt wird, in welche die variablen Daten entsprechend den im nichtflüchtigen Speicher NVM 5 bzw. im Kostenstellenspeicher gespeicherten Registerwerten eingefügt werden, ähnlich wie das bereits in den Spalten 1 bis 2 bzw. im Anspruch 9, in der deutschen Offenlegungsschrift DE 42 24 955, für die Bildung und Darstellung in drei mehrzeiligen Informationsgruppen bzw. für eine erforderliche Umschaltung in einen entsprechenden Modus prinzipiell ausgeführt wird. Wird eine gedrehte Darstellung verlangt, können entgegen den speziellen Ausführungen in der deutschen Offenlegungsschrift DE 42 24 955 A1, die Daten bereits im flüchtigen Speicher direkt so gedreht abgelegt werden, wie sie für den Druck benötigt werden. Die zeitaufwendige Routine des Drehens der Druckdaten wird nur einmalig für eine zusätzliche Bildpunktdatei bei der Programmierung des EPROMs beim Hersteller durchgeführt, was nur mehr Speicherplatz erfordert aber keine erhöhte Rechenleistung in der Frankiermaschine bindet.

Es ist bei einer anderen Variante weiterhin vorgesehen, daß auch variable Pixelbilddaten während des Druckens in die übrigen Pixelbilddaten eingebettet werden. Entsprechend der vom Encoder 13 gelieferten Positionsmeldung über den Vorschub der Postgutes bzw. Papierstreifens in Relation zum Druckermodul 1 werden die komprimierten Daten aus den Arbeitsspeichern 5a, 5b gelesen und mit Hilfe des Charakterspeichers 9 in ein binäre Pixeldaten aufweisendes Druckbild umgewandelt, welches ebenfalls in solcher dekomprimierten Form im flüchtigen Arbeitsspeicher 7 gespeichert wird. Nähere Ausführungen sind den europäischen Anmeldungen EP 576 113 A2 und EP 578 042 A2 entnehmbar.

Der Pixelspeicherbereich im Pixel-Speicher 7c ist also für die ausgewählten dekomprimierten Daten der festen Teile des Frankierbildes und für die ausgewählten dekomprimierten Daten der variablen Teile des Frankierbildes vorgesehen. Nach der Abrechnung erfolgt die eigentliche Druckroutine (im Schritt 406).

Wie aus der Figur 1 hervorgeht, stehen der Arbeitsspeicher 7b und der Pixelspeicher 7c mit dem Druckermodul 1 über eine ein Druckregister (P_{Reg}) 15 und eine Ausgabelogik aufweisende Druckersteuerung 14 in Verbindung. Der Pixelspeicher 7c ist ausgangsseitig an einen ersten Eingang der Druckersteuerung 14 geschaltet, an deren weiteren Steuereingängen Ausgangssignale der Mikroprozessorsteuereinrichtung 6 anlegen.

Sind alle Spalten eines Druckbildes gedruckt worden, wird wieder zur Systemroutine 200 zurückverzweigt.

Beim Übergang in die Systemroutine 200 wird - wie in der Figur 3 dargestellt - nach einem weiteren Schritt 201 zum Datenaufruf, insbesondere von Sleeping-Mode-Stückzahldaten, zunächst im Schritt 202 überprüft, ob die Kriterien für den Eintritt in den Sleeping-Mode erfüllt sind. Ist das der Fall wird zum Schritt 203

BNSDOCID <EP_____0762338A2_I_>

verzweigt, um mindestens eine Warnung mittels der Anzeigeeinheit 3 anzuzeigen. Dabei können weitere Schritte 204 bis 206 durchlaufen werden, bevor zum Schritt 209 verzweigt wird. Ist das aber nicht der Fall wird ebenfalls zum Schritt 209 verzweigt. Nach den Schritten wird in jedem Fall der Punkt t erreicht.

Nach erfolgter Neueingabe und Eingabe/Anzeige-Routine mit Druckdatenzusammenstellung und Aufruf der erforderlichen Bildpunktdateien im Schritt 209, wird unter der Voraussetzung, daß keine relevante Mängel festgestellt wurden, nun der Punkt e, d. h. der Beginn eines Kommunikationsmodus 300 erreicht. Dazu wird in einem Schritt 301 abgefragt, ob ein Transaktionsersuchen vorliegt. Ist das nicht der Fall, wird der Kommunikationsmodus 300 verlassen und der Punkt f, d.h. der Betriebsmodus 290 erreicht. Wurden relevante Daten im Kommunikationsmodus übermittelt, dann ist zur Datenauswertung auf den Schritt 213 zu verzweigen. Oder anderenfalls, wenn im Schritt 211 die Nichtübermittlung festgestellt wird, ist auf den Schritt 212 zu verzweigen. Nun wird überprüft, ob entsprechende Eingaben getätigt worden sind, um bei Testanforderung 212 in den Testmodus 216, anderenfalls um bei beabsichtigter Registerstandüberprüfung 214 in einen Anzeigemodus 215 zu gelangen. Ist das nicht der Fall, wird automatisch der Punkt d, d.h. der Frankiermodus 400 erreicht.

Erfindungsgemäß ist weiterhin vorgesehen, daß im Schritt 213 eine Statistik- und/oder Fehlerauswertung durchgeführt wird, um weitere aktuelle Daten zu gewinnen, welche nach Verzweigung zur Systemroutine 200 in Schritt 201 ebenfalls aufrufbar sind.
Wird der Punkt e, d.h. der Beginn des nachfolgend erläuterten Kommunikationsmodus 300 erreicht, wird im Schritt 301 abgefragt, ob ein Transaktionsersuchen vorliegt. Ein solches kann beispielsweise zur Guthaben- und Stückzahlnachladung oder Aktualisierung anderer relevanter Daten gestellt werden.

Der Benutzer wählt den Kommunikations- bzw. Fernwertvorgabemodus der Frankiermaschine über die Eingabe der Identifikationsnummer (achtstelligen Portoabrufnummer) und über die Betätigung der vorbestimmten T-Taste an. Ist der gewünschte Eingabeparameter richtig angezeigt, wird dies durch erneutes Betätigen der vorbestimmten T-Taste des Eingabemittels 2 bestätigt. Der Eingabeparameter wird bei Bedarf editiert. In der Anzeigeeinheit 3 erscheint dann eine Darstellung entsprechend der Eingabe.

Durch Betätigung der vorbestimmten T-Taste wird die Übertragung des Eingabeparameters über MODEM-Verbindung gestartet und die Eingabe überprüft. Der weitere Vorgang läuft automatisch ab, wobei der Ablauf durch eine entsprechende Anzeige begleitet wird.

Dazu prüft die Frankiermaschine, ob ein MODEM angeschlossen und betriebsbereit ist. Ist das nicht der Fall, wird auf den Schritt 310 verzweigt, um anzuzeigen, daß das Transaktionsersuchen wiederholt werden muß. Anderenfalls liest die Frankiermaschine die Wahlparameter, bestehend aus den Herauswahlparametern (Haupt-/Nebenstelle, usw.) und der Telefonnummer aus einem NVRAM-Speicherbereich F und sendet diese mit einem Wahlaufforderungskommando an das Modem 23. Anschließend erfolgt der für die Kommunikation erforderliche Verbindungsaufbau über das MODEM 23 mit der Datenzentrale Nach einer vorbestimmten Anzahl n ergebnisloser Wahlwiederholungen zwecks Verbindungsaufbau wird über einen Anzeigeschritt 310 auf den Punkt e zurückverzweigt.
Es ist vorgesehen, daß eine während der Kommunikation mit verschlüsselten Meldungen durchgeführte Transaktion einen Vorgabewert für einen Guthabennachladewert umfaßt, welcher der entfernten Datenzentrale übermittelt wird und/oder daß eine andere während der Kommunikation mit verschlüsselten Meldungen durchgeführte Transaktion eine spezifische Stückzahl S' für einen Sleeping-Mode umfaßt.

Eines der Transaktionsersuchen führt in der Frankiermaschine zu einer speziell gesicherten Guthabennachladung. Vorzugsweise erfolgt ein Absichern der außerhalb des Prozessors im Kostenstellenspeicher vorliegenden Postregister außerdem während der Guthabennachladung mittels einer Zeitsteuerung. Wird die Frankiermaschine beispielsweise mit einem Emulator/Debugger observiert, dann ist es wahrscheinlich, daß die Kommunikations- und Abrechnungsroutinen nicht innerhalb einer vorbestimmten Zeit ablaufen. Ist das der Fall, d.h. die Routinen benötigen erheblich mehr Zeit, würde dies in der Frankiermaschine erkannt und als Folge werden kritische Speicherbereiche unwiederbringlich gelöscht. Damit wird die Frankiermaschine am Weiterbetrieb gehindert.

Für die Übermittlung der für eine Guthaben- und/oder Stückzahlnachladung erforderlichen Daten sind relevante Schlüssel (Krypto-Keys) erforderlich, welche im Speicher in kryptifizierter Form abgelegt worden sind. Das Prinzip des Sicherungskonzeptes ist in den Figuren 12 und 13 dargestellt.

Vorzugsweise erfolgt eine Anwendung der DES-Algorithmus auf die für die Fernwertvorgabe benötigten Schlüssel, um diese in kryptifizierter Form abzulegen. Die Datenübertragung der Frankiermaschine zur Datenzentrale wird im Kommunikationsmodus 300 ebenfalls mit DES-Algorithmus abgesichert, wofür ein geheimer DES-Schlüssel benötigt wird. Dieser geheime DES-Schlüssel wird im Kommunikationsmodus 300 gebildet, indem die verschlüsselten Schlüssel während der Laufzeit der Frankiermaschine, d.h. während des Kommunikationsmodus 300 im OTP entschlüsselt werden, um einen geheimen Schlüssel KAct in den internen OTP-RAM zu laden.

Die Figur 12 zeigt die Eingabeverschlüsselung des Fernwertvorgabe DES-Schlüssels K_{Fix} zur Absicherung des Fernwertvorgabe DES-Schlüssels K_{Fix}. vor Manipulation.

Bei der Herstellung oder durch den Service-Techniker erhält jede Frankirmaschine über ihr Userinterface 2, 3 einen festen Fernwertvorgabeschlüssel K_{Fix}, der

BNSDOCID: <EP_____0762338A2_I_>

prinzipiell verborgen im NVRAM gehalten werden muß. Dafür wird der Fernwertvorgabeschlüssel im Schritt 60 mit der kryptographischen Funktion, Data-Encryption-Standard (**DES**), unter Verwendung des im OTP-ROM (Schritt 64) gespeicherten Geheimschlüssels K_{Kfix} verschlüsselt. Der verschlüsselte Geheimschlüssel K_{Fix} wird nun im externen Datenspeicher (NVRAM) abgelegt.

In der Figur 13 ist dargestellt, welche Schritte zur Laufzeit der Frankiermaschine für eine Fernwertvorgabe durchgeführt werden müssen, damit aus dem verschlüsselten K_{Fix}-Wert im externen NVRAM der DES-Schlüssel *KAct* gebildet wird, der für die Zeit der Fernwertvorgabeprozedur im prozessorinternen RAM gehalten wird. Der Geheimschlüssel K_{Kfix} wird dem internen OTP-ROM (Block 64) und verschlüsselte Schlüssel Crypt K_{Fix} wird dem NVRAM entnommen Der Block 60 der Figur 13 zeigt die Entschlüsselung DES-Schlüssels K_{Fix} und eine Speicherung im internen OTP-RAM für die Fernwertvorgabe im Block 65.

Die Frankiermaschine führt regelmäßig und/oder beim Einschalten den Registercheck durch und kann somit die fehlende Information erkennen, falls die Maschine unautorisiert geöffnet worden war. Die Frankiermaschine wird dann blockiert.

Der potentielle Manipulator einer Frankiermaschine muß mehrere Schwellen überwinden, was natürlich einen gewissen Zeitaufwand bedarf. Erfolgt in gewissen Zeitabständen keine Verbindungsaufnahme von der Frankiermaschine zur Datenzentrale, wird die Frankiermaschine bereits suspekt. Es ist dabei davon auszugehen, daß derjenige, der eine Manipulation an der Frankiermaschine begeht, sich kaum wieder bei der Datenzentrale melden wird.

Die Steuereinrichtung 6 weist einen Mikroprozessor oder einen OTP auf. Im OTP sind neben einem Mikroprozessor auch nichtflüchtige Speicher und weitere Schaltungen in einem gemeinsamen Gehäuse untergebracht. Der interne nichtflüchtige Speicher umfaßt beispielsweise Programmspeicher und insbesondere auch die Möglichkeit Sicherungsbits zu setzen, die das Auslesen des internen nichtflüchtigen Speichers von außen verhindern. Diese Sicherungsbits werden während der Herstellung der Frankiermaschine im OTP gesetzt. Das Observieren solcher sicherheitsrelevanter Routinen, wie beispielsweise Abrechnungsroutinen, mit einem Emulator/ Debugger würde ebenfalls zu einem veränderten Zeitablauf führen, was durch den OTP feststellbar ist. Dieser umfaßt auch eine Taktgeber/Zähler-Schaltung für die Vorgabe von Zeitintervallen bzw. Taktzyklen beispielsweise für die Time-out-Generierung oder Druckersteuerung. Wenn eine bestimmte Zeit abgelaufen ist und das erwartete Ereignis nicht eingetreten ist, wird vom der Taktgeber/Zähler-Schaltung ein Interrupt generiert, der dem Mikroprozessor den ergebnislosen Ablauf der Zeitspanne meldet, woraufhin der Mikroprozessor weitere Maßnahmen veranlaßt. Erfindungsgemäß wird die Taktgeber/Zähler-Schaltung für eine Programmlaufzeitüberwachung eingesetzt. Dabei wird von einer bekannten Anzahl von Taktzyklen für den Programmablauf von vorbestimmten Programmteilen ausgegangen. Vor dem Start der Routine wird der Zähler der Taktgeber/Zähler-Schaltung in vorbestimmter Weise voreingestellt bzw. zurückgesetzt. Nach dem Start der Programmroutine wird entsprechend den Taktimpulsen des Taktgebers der Zählerstand laufend verändert. Nach Abarbeitung der kritischen vorbestimmten Programmteile wird der Zustand des Zählers vom Mikroprozessor abgefragt und mit dem erwarteten Wert verglichen. Beim Überschreiten einer vorbestimmten Abweichung in der Laufzeit kritischer bzw. sicherheitsrelevanter Programmteile kann die Frankiermaschine somit nicht weiter zum Frankieren betrieben werden (Kill Mode 1). Nimmt ein Manipulator einen unautorisierten Eingriff vor, wird die Frankiermaschine während der Laufzeit durch das Überführen in den ersten Modus wirksam außer Betrieb gesetzt.

Bei einer Inspektion werden die Registerstände überprüft. Bei Bedarf kann ein Probeabdruck mit dem Wert 0 gemacht werden. Bei einer Reparatur durch den Service vor Ort muß eventuell in die Frankiermaschine eingegriffen werden. Die Fehlerregister sind beispielsweise mit Hilfe eines speziellen Service-EPROM auslesbar, welches an die Stelle des Advert-EPROM gesteckt wird. Wenn auf diesen EPROM-Steckplatz vom Prozessor nicht zugegriffen wird, wird gewöhnlich ein Zugriff auf die Datenleitungen durch spezielle - in der Figur 2 dargestellte - Treiberschaltkreise (Buffer) verhindert. Die Datenleitungen, welche hier durch eine unversiegelte Gehäusetür erreichbar sind, können somit nicht unbefugt kontaktiert werden. Eine andere Variante ist das Auslesen von Fehlerregisterdaten durch einen über eine Schnittstelle angeschlossenen Service-Computer, wobei die Schnittstelle dann entsprechende Sicherheitsmaßnahmen aufweisen muß.

Es ist außerdem auch in Zeiten in welchen nicht gedruckt wird (Standby Modus) vorgesehen, daß eine Abfrage hinsichtlich Manipulationsversuchen erfolgt und/ oder die Checksumme der Registerstände und/oder über den Inhalt des Programmspeichers PSP 11 gebildet wird. Zur Verbesserung der Manipulationssicherheit wird dabei für einen Kill-Mode 2 die Checksumme im OTP über den Inhalt des externen Programmspeichers PSP 11 gebildet und das Ergebnis mit einem im OTP gespeicherten vorbestimmten Wert verglichen. Dies erfolgt vorzugsweise im Schritt 101, wenn die Frankiermaschine gestartet wird, oder im Schritt 213, wenn die Frankiermaschine im Standby-Modus betrieben wird. Der Standby-Modus wird erreicht, wenn eine vorbestimmte Zeit keine Eingabe- bzw. Druckanforderung erfolgt. Letzteres ist der Fall, wenn ein an sich bekannter - nicht näher dargestellter - Briefsensor keinen nächsten Briefumschlag ermittelt, welcher frankiert werden soll. Der - in der Figur 5 gezeigte - Schritt 405 im Frankiermodus 400 umfaßt daher noch eine weitere Abfrage nach einem Zeitablauf, welche bei Zeitüberschreitung letztendlich wieder auf

BNSDOCID <EP_____0762338A2 I_>

den Punkt t und damit auf die Eingaberoutine gemäß Schritt 209 führt. Wird das Abfragekriterium erfüllt, wird wie im Schritt 408 ein Standby-Flag gesetzt und direkt auf den Punkt s zur Systemroutine 200 oder zum Punkt t zurückverzweigt, ohne daß die Abrechnungs- und Druckroutine im Schritt 406 durchlaufen wird. Das Standby-Flag wird später im Schritt 211 abgefragt und nach der Checksummenprüfung im Schritt 213 zurückgesetzt, falls kein Manipulationsversuch erkannt wird.

Das Abfragekriterium in Schritt 211 wird dazu um die Frage erweitert, ob das Standby-Flag gesetzt ist, d.h. ob der Standby Modus erreicht ist. In diesem Fall wird ebenfalls auf den Schritt 213 verzweigt. Der Vorteil dieses Verfahrens in Verbindung mit dem ersten Modus besteht darin, daß der Manipulationsversuch statistisch im Schritt 213 erfaßt wird.

Um die Sicherheit gegenüber Manipulationen weiter zu erhöhen wird erfindungsgemäß eine Flußkontrolle (Flow Control) eingesetzt, welche nachfolgend erläutert wird. Eine solche Flow Control erfolgt durch Verändern eines Zählwertes in einem Speicher an mindestens einem Punkt während der Ausführung der Programmroutine. Nach Ausführung der Programmroutine wird der veränderte Zählwert mit einem dieser Programmroutine zugeordneten vorbestimmten Zählwert verglichen. Werden nun während der Programmausführung Verzweigungen durchlaufen, so können sich unterschiedliche Zählwerte ergeben. In einer nachfolgenden Auswertung wird ein Plausibilitätstest durchgeführt bzw. es kann festgestellt werden, welche Verzweigungen durchlaufen wurden. Das ist dadurch möglich, da die Veränderung des Zählwertes durch eine Multiplikation mit einer bestimmten dem jeweiligen Programmteil zugeordneten Primzahl erfolgt. Bei einer späteren Auswertung muß dann lediglich eine Primzahlzerlegung durchgeführt werden.

In einer anderen Variante, wo nur solche Programmteile ohne Verzweigungen berücksichtigt werden bzw. keine Rückverfolgung der durchlaufenen Programmzweige erforderlich wird, ist ein Inkrementieren des Zählwertes und abschließender Vergleich mit mindestens einem vorbestimmten Zahlwert ausreichend.

Der in der Figur 3 dargestellte Gesamtablaufplan für ein Sicherheitssystem weist Schritte 201 bis 206 für eine Überwachung weiterer Kriterien auf. Bei einer Verletzung eines der Sicherheitskriterien tritt die Frankiermaschine in einen Sleeping-Modus ein, beispielsweise, wenn nach Verbrauch einer vorbestimmten Stückzahl noch keine Verbindung zur Datenzentrale aufgenommen wurde.

Die Frankiermaschine und die Datenzentrale verabreden jeweils eine vorbestimmte Stückzahl S, d.h. die Menge, die bis zur nächsten Verbindungsaufnahme frankiert werden kann. Falls eine Kommunikation nicht zustande kommt (Stückzahlkontrolle), verlangsamt die Frankiermaschine ihre Arbeitsweise (Sleeping Modus-Variante 1).

Eine andere Variante gibt eine ständige Warnung für ein bevorstehendes Schlafenlegen der Frankierfunktion im Schritt 203 aus, wobei dieser nun aufgrund des erfüllten Abfragekriteriums in Schritt 202 ständig durchlaufen werden muß, bevor Schritt 205 erreicht wird. Es ist weiterhin vorgesehen, daß der Schritt 203 einen Subschritt zur Fehlerstatistik entsprechend dem Statistik- und Fehlerauswertungsmodus 213 umfaßt.

Die Frankiermaschine verlangt in der aus US 3 255 439 bekannten Weise eine Verbindung zur Datenzentrale. Kommt die Verbindung zustande, prüft die Datenzentrale die Registerstände. Falls die Nachladung nicht vorgenommen werden kann, hindert die Datenzentrale durch ein zur Frankiermaschine übermitteltes Signal diese am weiteren Betrieb. Wenn die Verbindung kurz nach der von der Frankiermaschine vorgenommenen Signalisierung zustande kam und die Registerstände nicht bemängelt werden, kann die Frankiermaschine ohne eine weitere außerordentliche Inspektion in den Betriebsmodus zurückgeschaltet werden. Hierzu werden neue aktuelle Daten beispielsweise für ein Guthaben und für die erlaubte Stückzahl übermittelt, welche bis zur nächsten Verbindungsaufnahme frankiert werden kann.

Die Datenzentrale kann aufgrund des übermittelten Signalisierungscodes zwischen automatisch vorgenommener und normaler Kommunikation unterscheiden. Erstere wird immer dann erfolgen, wenn der Nutzer der Frankiermaschine die Aufforderungen zur Kommunikation übersehen bzw. ignoriert hat und entsprechende Eingabehandlungen unterläßt. Hierbei kann im Wiederholungsfall bei einem Verdacht einer Manipulation eine Sonderinspektion angeordnet werden.

Vom Frankiermodus kann dann direkt auf den Kommunikationsmodus 300 Punkt e zurückverzweigt werden. Damit können weiterhin auch andere Eingaben, beispielsweise gemäß den Schritten Testanforderung 212 oder Registercheck 214 getätigt werden. Nur falls auf den Frankiermodus 400 verzweigt wird, wird dann im Schritt 410 entsprechend dem Entscheidungskriterium erneut festgestellt, ob eine automatische Kommunikation erforderlich ist. Das ist vorzugsweise der Fall, falls die vorbestimmte Stückzahl verbraucht ist.

War die Kommunikation erfolgreich und wurden Daten übermittelt (im Schritt 211 abgefragt), wird ebenfalls der Schritt 213 erreicht. Im Schritt 213 werden die aktuellen Daten ermittelt bzw. geladen, welche im Schritt 201 aufgerufen und anschließend wieder beim Vergleich im Schritt 202 benötigt werden. Das übermittelte Entscheidungskriterium ist vorzugsweise die neue Stückzahl S'.

Eine alternative Variante besteht darin, daß das Entscheidungskriterium das neue zum Frankieren übermittelte Guthaben ist und im Auswertemodus 213 die neue Stückzahl S' intern in der Frankiermaschine ermittelt wird. Die Kommunikation mit der Datenzentrale umfaßt in diesem Fall nicht mehr die neue Stückzahl S', sondern ist lediglich zur Auslösung der Berechnung im Auswertemodus 213 erforderlich. Die Berechnung erfolgt intern in der Frankiermaschine und gleichzeitig parallel dazu in der Datenzentrale nach den gleichen

BNSDOCID: <EP_____0762338A2_I_>

Methoden aufgrund der übermittelten Registerdaten.

Die Frankiermaschine kann der Datenzentrale Registerwerte vor einer Guthabennachladung übermitteln:

R1 (descending register) vorrätige Restbetrag in der Frankiermaschine,
R2 (ascending register) Verbrauchssummenbetrag in der Frankiermaschine,
R3 (total resetting) die bisherige Gesamtvorgabesumme aller Fernwertvorgaben,
R4 (piece count Σprinting with value =/=0) Anzahl gültiger Drucke,
R8 (R4 + piece count Σprinting with value =0) Anzahl aller Drucke daraus folgt:

$$R3 = R2 + R1 \quad (1)$$

Bei jeder Fernwertvorgabe läßt sich R1 abfragen und statistisch auswerten. Wird R1 immer größer, dann kann der gleiche Nachladebetrag in immer größeren Nachladeperioden nachgeladen werden, bzw. die Stückzahl wird kleiner angesetzt, welche bis zur nächsten Kommunikation frankiert werden darf.

Anhand der frankiermaschinenspezifischen Daten läßt sich ein Frankiermaschinen-Profil erstellen. Dieses Frankiermaschinen-Profil gibt darüber Auskunft, ob ein Kunde mit den durchgeführten Nachladevorgängen in der Lage war, die ermittelte Anzahl an Frankierungen durchzuführen. Es sind innerhalb des Suspicious Mode zwei Stufen zu unterscheiden:

1. Frankiermaschine ist verdächtig und
2. Frankiermaschine muß manipuliert worden sein.

In regelmäßigen Abständen wird in der Datenzentrale eine Plausibilitätskontrolle sämtlicher im Einsatz befindlicher Frankiermaschinen durchgeführt. Bei diesem Verfahren werden die Maschinen gekennzeichnet und der Postbehörde gemeldet, deren Frankierverhalten verdächtig erscheinen oder manipuliert worden sind. In der Frankiermaschine ist ggf. noch eine andere Sicherheitsmaßnahme (Error Overflow Mode) vorgesehen. Diese kann im zweiten Modus neben oder anstatt der Sleeping-Mode-Variante 1 oder Sleeping-Mode-Variante 2 durchgeführt werden. Bei Erfüllung des Abfragekriteriums im Schritt 202, d.h. bei Überschreitung einer vorbestimmten Anzahl an Fehlern, verlangsamt sich die Reaktionszeitdauer der Frankiermaschine im Schritt 203, wobei über die Anzeige gleichzeitig dieser Zustand an den Bediener der Frankiermaschine gemeldet wird. In den weiteren Schritten kann ähnlich verfahren werden, wie in Zusammenhang mit den Figuren 2 und 5 bereits erläutert wurde. Die Frankiermaschine speichert sowohl interne als auch Bedienungsfehler und Manipulationsversuche in einem Fehlerregister zu protokollarischen Zwecken beispielsweise bis zu der Zahl 999. Wird der Zustand der Überschreitung der Fehleranzahl nicht beseitigt, beispielsweise im Rahmen einer Inspektion durch einen Servicedienst oder durch Rücksetzen während einer Kommunikation mit der Datenzentrale, kann die Reaktionszeitdauer weiter erhöht werden, um eventuelle Manipulationen zu erschweren. Die Fehlerzahl wird dann weiter d.h. wieder bis zu einer vorbestimmten Zahl, beispielsweise im Schritt 213 protokolliert.

In einer ersten Variante ist vorgesehen, die Reaktionszeitdauer, beispielsweise die Zeitdauer bis zum Beginn des Druckbetriebes, linear mit der Anzahl der Fehler zu erhöhen. Die Ausführung des Programmes wird dadurch weder modifiziert noch verhindert, sondern nur verzögert. Insbesondere werden solche unkritischen Programmteile, welche nicht durch Time supervision (Kill Mode 1) oder Flow control überwacht werden, mehrfach aufgerufen, wie beispielsweise die Fehleranzeige. Damit bleibt die Wirkung des Programmes im wesentlichen unverändert.

In einer zweiten Variante wird die Reaktionszeitdauer jeweils um eine Stufe erhöht, wobei die Stufen Sekunden, Minuten, Stunden, Tage, ... usw. betreffen können.

In Abänderung bzw. in Kombination mit vorgenannten Varianten kann eine Erhöhung der Reaktionszeitdauer außerdem bei jeder Fehlbedienung vorgesehen werden. Hierzu wird in einer Ausführungsform ein elektronisches Zeitschloß betätigt. Vorzugsweise wird eine progressive Steigerung der Reaktionszeitdauer im Betriebsprogramm vorgesehen, um eine Manipulation zu erschweren.

Es ist vorgesehen, daß der Schritt 213 teilweise oder ganz in Verbindung mit anderen Schritten als Subschritt aufgerufen wird. Beispielsweise ist der Statistik und Fehlermodus Bestandteil des Schrittes 203 und der Abrechnungs- und Druckroutine gemäß des Schrittes 406 im Frankiermodus 400, welcher in den Figuren 3 und 5 näher dargestellt ist. Tritt ein schwerer Abrechnungsfehler auf wird die Maschine im Schritt 406 blokkiert. Tritt ein Fehler aber während der Initialisierungsphase im Schritt 101 auf, bleibt die Maschine unter Anzeige eines bestimmten Fehlercodes stehen.

Andererseits gibt es schwere Fehler, welche erst anläßlich der nächsten Inspektion vor Ort von einer dazu berechtigten Person aufgehoben werden können. Ein solcher Fehler, beispielsweise wenn der Prozessor nicht auf den Arbeitsspeicher zugreifen kann, d.h. den Dateninhalt des RAM's weder lesen noch verändern kann, wird beispielsweise durch Stecken eines speziellen RESET-EPROM's beseitigt. Hierzu muß die Verplombung der Klappe und die Frankiermaschine geöffnet werden. Das RESET-EPROM enthält die erforderlichen Daten, beispielsweise den entsprechenden Schlüssel, und spezielle Programme zur Wiederherstellung der Frankiermaschinenfunktion. Beispielsweise kann ein solches Programm eine erfolgte Redundanzverringerung wieder rückgängig machen. Die Protokollierung der Fehler, welche während des Betriebes der Frankiermaschine im Statistik- und Fehlerauswertungs-

BNSDOCID <EP_____0762338A2_I >

modus (Schritt 213) getrennt nach Fehlerarten erfolgt, wird dabei von der berechtigten Person daraufhin überprüft, ob ein Manipulationsversuch unternommen worden ist.

Die Erfindung ist nicht auf die vorliegenden Ausführungsformen beschränkt. Vielmehr ist eine Anzahl von Varianten denkbar, welche von der dargestellten Lösung auch bei grundsätzlich anders gearteten Ausführungen Gebrauch machen.

Patentansprüche

1. Verfahren zur Absicherung von Daten und Programmcode einer elektronischen Frankiermaschine mit einem Mikroprozessor in einer Steuereinrichtung der Frankiermaschine zur Ausführung von Schritten für eine Start- und Initialisierungsroutine und nachfolgender Systemroutine mit einer Möglichkeit in einen Kommunikationsmodus mit einer entfernten Datenzentrale einzutreten sowie weiteren Eingabeschritten, um in einen Frankiermodus einzutreten von dem nach Ausführung einer Abrechnungs- und Druckroutine in die Systemroutine zurückverzweigt wird, wobei in den Schritten für die Start- und Initialisierungsroutine ein Übertragen eines extern gespeicherten vorbestimmten MAC-Wertes und ausgewählter Daten eines zu prüfenden Speicherinhaltes in einen Speicher der Frankiermaschine, ein Bilden einer MAC-Prüfsumme im OTP-Prozessor über den Inhalt desjenigen externen Speichers, welchem der MAC zugeordnet ist, eine Überprüfung auf Gültigkeit der Daten mittels eines ausgewählten Prüfsummenverfahrens innerhalb eines Prozessors durchgeführt wird, um bei Gültigkeit ein Frankieren zu erlauben, **gekennzeichnet durch**

   a) Übertragen eines extern gespeicherten vorbestimmten MAC-Wertes und ausgewählter Daten und Programmcode eines zu prüfenden Speicherinhaltes in den internen OTP-RAM zur flüchtigen Speicherung und ein Bilden einer MAC-Prüfsumme im OTP-Prozessor über den Inhalt desjenigen externen Speichers, welchem der MAC zugeordnet ist, für eine Startsicherheitsüberprüfung (1020) im Rahmen der Start- und Initialisierungsroutine (101), welche abläuft vor einer sicheren Druckdatenaufrufroutine (1040) und der nachfolgenden Systemroutine (200), zur Feststellung der Gültigkeit eines gültigen Programm-Code und von gültigen Daten im vorbestimmten Speicherplatz, wobei ein zugehöriger MAC (MESSAGE AUTHENTIFICATION CODE) im selben Speichermittel gespeichert vorliegt und wobei die Überprüfung auf gültigen Programm-Code und auf Gültigkeit der Daten mittels eines ausgewählten Prüfsummenverfahrens innerhalb eines OTP-Prozessors (ONE TIME PROGRAMMABLE) durchgeführt wird, der intern die entsprechenden Programmteile, einen Verschlüsselungs-Algorithmus und einem zugehörigen Schlüssel enthält und

   b) Überführung der Frankiermaschine in die vorgenannte Systemroutine (200) und Übertragen eines extern gespeicherten vorbestimmten MAC-Wertes und ausgewählter Daten und Programmcode eines zu prüfenden Speicherinhaltes in den internen OTP-RAM zur flüchtigen Speicherung und ein Bilden einer MAC-Prüfsumme im OTP-Prozessor über den Inhalt desjenigen externen Speichers, welchem der MAC zugeordnet ist, für eine kontinuierliche Überprüfung in jedem Durchlauf der Betriebsprogrammschleife, wobei vorschreitend über jeweils eine größere Anzahl von Programmspeicherzellen mittels eines kryptographischen Prüfsummenverfahrens ein relevanter MAC gebildet und mit dem jeweiligen gespeicherten, zum Zeitpunkt T1 gebildeten MAC verglichen werden kann,

   c) Ablaufen von Programmen, wobei alle wesentlichen Programmabläufe in das Innere des OTP-Prozessors verlegt ablaufen, wobei ein Überführung der Frankiermaschine in einen ersten Modus, wenn mindestens ein überprüftes Programm ungültig ist bzw. ein spezifisches Manipulationskriterium erfüllt ist, durch Schritte zum Verhindern des Frankierens bzw. Sperrens der Frankiermaschine und/oder Schritte zum Verhindern einer weiteren Programmausführung bzw. einer vom OTP-Prozessor nach extern führenden Programmverzweigung im Rahmen vorgenannter Systemroutine (200), und

   d) Wiederholung der Prüfung der Frankiermaschine auf Vorliegen einer Manipulation im Rahmen vorgenannter Systemroutine (200).

2. Verfahren, nach Anspruch 1, **dadurch gekennzeichnet**, daß als ein spezifisches Manipulationskriterium das Intervall zwischen den Prüfsummenvergleichen mit einer zeitlichen Überwachung verknüpft wird, so daß ein Anhalten des Programms erkannt wird.

3. Verfahren nach den Ansprüchen 1 bis 2, **dadurch gekennzeichnet**, daß die Frankiermaschine nach Zeitablauf ohne Frankierauslösung und/oder nach einer Anzahl von Programmschleifen-Durchläufen ohne Eingabe im Standby-Modus betrieben wird, wobei im Standby-Modus Sicherheitsüberprüfungen sicherheitsrelevanter Daten und Programme durchgeführt werden und im Fehlerfall eine Protokollierung und anschließende Blockierung der Frankiermaschine erfolgt.

4. Verfahren nach einem der vorgenannten Ansprü-

BNSDOCID: <EP_____0762338A2_I_>

che 1 bis 3, **dadurch gekennzeichnet**, daß eine Authentizitätsprüfung von mindestens den wesentlichsten Teilen des Programmcodes und den wesentlichsten Daten in Speicherbereichen eines Klischee-EPROM oder eines anderen externen EPROMs durchgeführt wird.

5. Verfahren, nach Anspruch 1, **dadurch gekennzeichnet**, daß nach einer Gültigkeitsprüfung die Frankiermaschine in einen zweiten Modus überführt wird, wenn ein spezifisches Kriterium erfüllt ist, wobei die Schritte (201 bis 206), die nach dem Beginnpunkt s der Systemroutine (200) und vor dem Punkt t ablaufen, umfassend:

- einen Schritt (201) zum Aufruf aktueller Daten
- einen Schritt (202) zur Überprüfung der Daten mittels eines Entscheidungskriteriums und Eintritt bei Erfüllung des Kriteriums in den zweiten Modus (Schritte 203-206), um an den Benutzer der Frankiermaschine eine Warnung und Aufforderung zur Kommunikation mit der Datenzentrale abzugeben sowie gekennzeichnet durch eine Durchführung von Authentizitätsprüfungen in mindestens einem weiteren Modus, wobei zur Bildung des MAC ein im internen OTP-ROM sicher gespeicherter DES-Algorithmus zur Verschlüsselung verwendet wird und daß zugehörige Schlüssel im internen OTP-ROM sicher gespeichert vorliegen, wobei ein Schlüssel für die Absicherung aller Speicherinhalte oder eine Anzahl verschiedener Schlüssel für die Absicherung der unterschiedlichen Speicherinhalte verwendet wird.

6. Verfahren, nach Anspruch 5, **dadurch gekennzeichnet**, daß der zweite Modus (Sleeping-Mode) eine Warnung vor der bevorstehenden automatischen Durchführung einer Kommunikation mit der Datenzentrale umfaßt und daß eine Authentizitätsprüfung von Registerwerten aus den Speicherbereichen eines nichtflüchtigen Speichers (NVRAM, EEPROM) bei der Startsicherheitsüberprüfung (1020) **und** im Frankiermodus durchgeführt wird.

7. Verfahren, nach Anspruch 6, **dadurch gekennzeichnet**, daß für die Kommunikation mit einer Datenzentrale ein geheimer erster Schlüssel eingesetzt wird, der im nichtflüchtigen Speicher extern vom OTP-Prozessor in verschlüsselter Form gespeichert vorliegt, der mittels eines internen zweiten Schlüssels innerhalb des OTP-Prozessors entschlüsselt wird, daß der verschlüsselte erste Schlüssel in Verbindung mit dem DES-Algorithmus und dem vorgenannten zweiten Schlüssel entschlüsselt wird, welche im internen OTP-ROM sicher gespeichert vorliegen, daß der entschlüsselte erste Schlüssel in Verbindung mit dem DES-Algorithmus zur Sicherung der Kommunikation der Frankiermaschine mit der Datenzentrale eingesetzt wird.

8. Verfahren nach Anspruch 7, **gekennzeichnet dadurch**, daß während der Kommunikation Transaktionen mit verschlüsselten Meldungen durchgeführt werden, um ein Guthaben und/oder weitere aktuelle Daten in die Frankiermaschine zu laden, sowie daß die Transaktionsdaten einzeln und seriell übertragen und durch einen MESSAGE AUTHENTIFICATION CODE (MAC) gesichert werden, wobei die MAC-Bildung intern im OTP-Prozessor erfolgt.

9. Verfahren, nach Anspruch 8, **dadurch gekennzeichnet**, daß eine während der Kommunikation mit verschlüsselten Meldungen durchgeführte Transaktion einen Vorgabewert für einen Guthabennachladewert umfaßt, welcher der entfernten Datenzentrale übermittelt wird.

10. Verfahren, nach Anspruch 8, **dadurch gekennzeichnet**, daß eine während der Kommunikation mit verschlüsselten Meldungen durchgeführte Transaktion eine spezifische Stückzahl S' für den Sleeping-Mode umfaßt.

11. Verfahren nach einem der vorgenannten Ansprüche 1 bis 10, **dadurch gekennzeichnet**, daß im Betriebsmodus (290) ein Schritt (214) für eine Umschaltung in einen Anzeigemodus (215) zur Anzeige von Registerwerten zum Zwecke Ihrer Überprüfung vorgesehen ist, wobei zu Kontrollzwecken wahlweise Registerwerte mit dem frankiermaschinen-internen Drucker ausgedruckt werden können.

12. Verfahren nach einem der vorgenannten Ansprüche 1 bis 11, **dadurch gekennzeichnet**, daß alle wesentlichen Programmabläufe in das Innere des OTP-Prozessors verlegt ablaufen und daß die Frankiermaschine auf Vorliegen einer Manipulation wiederholt geprüft wird.

13. Verfahren zur Absicherung von Daten und Programmcode einer elektronischen Frankiermaschine gegen Manipulation mit einem Mikroprozessor in einer Steuereinheit der Frankiermaschine zur Ausführung von Schritten für eine Start- und Initialisierungsroutine und nachfolgender Systemroutine mit einer Möglichkeit in einen Kommunikationsmodus mit einer entfernten Datenzentrale einzutreten sowie weiteren Eingabeschritten, um in einen Frankiermodus einzutreten von dem nach Ausführung einer Abrechnungs- und Druckroutine in die Systemroutine zurückverzweigt wird, **gekennzeichnet durch**

a) eine Startsicherheitsüberprüfung (1020) im

BNSDOCID <EP_____0762338A2_I_>

Rahmen einer Start- und Initialisierungsroutine (101), welche abläuft vor einer sicheren Druckdatenaufrufroutine (1040) und der nachfolgenden Systemroutine (200), zur Feststellung der Gültigkeit eines Programm-Codes und/oder von Daten im vorbestimmten Speicherplatz und eines zugehörigen MAC (MESSAGE AUTHENTIFICATION CODE), welche im selben Speichermittel gespeichert vorliegen, wobei die Überprüfung auf gültigen Programm-Code und/oder auf gültige Daten mittels eines ausgewählten Prüfsummenverfahrens innerhalb eines OTP-Prozessors (ONE TIME PROGRAMMABLE) durchgeführt wird, der intern die entsprechenden Programmteile enthält und

b) Überführung der Frankiermaschine in die vorgenannte Systemroutine (200) bei Gültigkeit der Daten oder Überführung der Frankiermaschine in einen ersten Modus, wenn die Daten ungültig sind bzw. ein spezifisches Manipulationskriterium erfüllt ist, durch Schritte zum Verhindern des Frankierens bzw. Sperrens der Frankiermaschine (1030) und/oder Schritte zum Verhindern einer weiteren Programmausführung bzw. einer vom OTP-Prozessor nach extern führenden Programmverzweigung im Rahmen vorgenannter Systemroutine (200).

c) Durchführung von Authentizitätsprüfungen im Ergebnis der Druckdateneingabe in der Druckdatenaufrufroutine (1040) für Rahmen und/oder Fensterdaten während der Start- und Initialisierungsroutine (101) und im Schritt (209) für sicherheitsrelevante Fensterdaten, welche bei der Druckdateneingabe geändert wurden, wobei bei fehlender Authentizität Schritte zum Verhindern einer weiteren Programmausführung bzw. einer vom OTP-Prozessor nach extern führenden Programmverzweigung im Rahmen vorgenannter Systemroutine (200) und wobei bei bestehender Authentizität Schritte zur weiteren Programmausführung im Rahmen vorgenannter Systemroutine (200) durchgeführt werden.

14. Verfahren zur Absicherung von Daten und Programmcode einer elektronischen Frankiermaschine gegen Manipulation mit einem Mikroprozessor in einer Steuereinheit der Frankiermaschine zur Ausführung von Schritten für eine Start- und Initialisierungsroutine und nachfolgender Systemroutine mit einer Möglichkeit in einen Kommunikationsmodus mit einer entfernten Datenzentrale einzutreten sowie weiteren Eingabeschritten, um in einen Frankiermodus einzutreten von dem nach Ausführung einer Abrechnungs- und Druckroutine in die Systemroutine zurückverzweigt wird,
gekennzeichnet durch

a) eine Startsicherheitsüberprüfung (1020) im Rahmen einer Start- und Initialisierungsroutine (101), welche abläuft vor einer sicheren Druckdatenaufrufroutine (1040) und der nachfolgenden Systemroutine (200), zur Feststellung der Gültigkeit eines Programm-Codes und/oder von Daten im vorbestimmten Speicherplatz,

b) Überführung der Frankiermaschine in die vorgenannte Systemroutine (200) bei Gültigkeit der Daten oder Überführung der Frankiermaschine in einen ersten Modus, wenn die Daten ungültig sind bzw. ein spezifisches Manipulationskriterium erfüllt ist,

c) kontinuierliche Programmüberwachung innerhalb der Systemroutine (200) und Überführung der Frankiermaschine in den ersten Modus, wenn die Daten ungültig sind bzw. ein spezifisches Manipulationskriterium erfüllt ist, wobei über jeden der Subblöcke SB eines Blocks B eine Prüfsumme oder MAC inkrementell berechnet wird, wobei eine kumulierte Prüfsumme bzw. MAC gebildet und ein Vergleich mit einem früher gespeicherten Wert für vorgenannte Prüfsumme bzw. MAC vorgenommen wird, um die Authentizität der Programmteile voranschreitend festzustellen.

15. Verfahren, nach Anspruch 14, **gekennzeichnet** durch die Schritte:

- Aufrufen der Codewörter des jeweiligen Subblocks SB des aktuellen Blocks B im Schritt (210-1), um darüber insgesamt eine Prüfsumme oder mittels DES-Verschlüsselung einen MAC zu bilden, wobei die Prüfsummen- bzw. die MAC-Berechnung für einen ganzen Block unterbrochen und im nächsten Durchlauf weitergeführt wird und wobei die Prüfsumme bei jedem Durchlauf kumuliert und dann gegebenenfalls wieder der inkrementell MAC gebildet wird,
- Vorsehen eines Schrittes (210-2) zum Inkrementieren des Subblockzählers, um fortschreitend im nächsten Durchlauf wieder im Schritt (210-1) kumulieren zu können und um dann den jeweiligen inkrementellen MAC zu bilden, wobei nach dem Schritt (210-2) zum Inkrementieren des Subblockzählers über einen Prüfschritt (210-3) zum Punkt e der Systemroutine verzweigt wird, wenn der maximale Subblockzählerstand SBZmax noch nicht erreicht ist, oder wobei, wenn Endstand bei der Prüfsummenbildung bzw. bei der MAC-Bildung erreicht ist, nach dem Prüfschritt (210-3) in einem weiterem Schritt (210-4) die vorgenannte kumulierte Prüfsumme bzw. der MAC mit einem zugehörig gespeicherten Wert verglichen wird, wobei im nachfolgenden Prüfschritt (210-5) festgestellt wird, ob eine Identität oder ein Fehler vorliegt,

BNSDOCID: <EP_____0762338A2_I_>

- Verzweigen im Fehlerfall, wobei Flag gesetzt, welches in einem Schritt (409) des Frankiermodus (400) ausgewertet wird, oder
- Abschluß der Autentifizierung und Durchführung eines Schrittes (210-6) zur Blockinkrementation und eines Schrittes (210-7) zur Rücksetzung des Subblockzählerstandes (SBZ := 0) und der Prüfsumme auf den Wert Null, Prüfen im Schritt (210-8), ob alle Blöcke abgearbeitetet wurden, um den Blockzähler im Schritt (210-9) wieder auf den ersten Block zu setzten (BZ := 0) und Verzweigung auf den Punkt e zur weiteren Abarbeitung der Systemroutine.

BNSDOCID <EP_____0762338A2_I_>

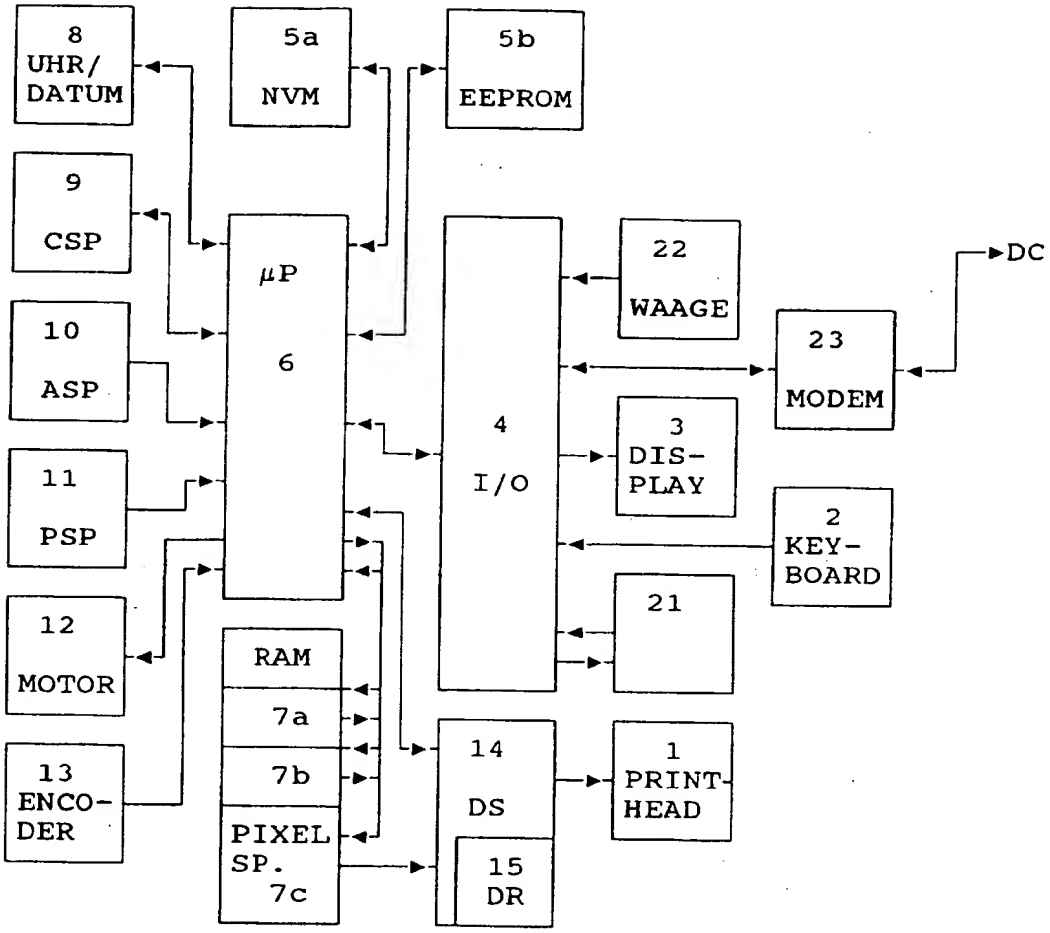

Fig. 1

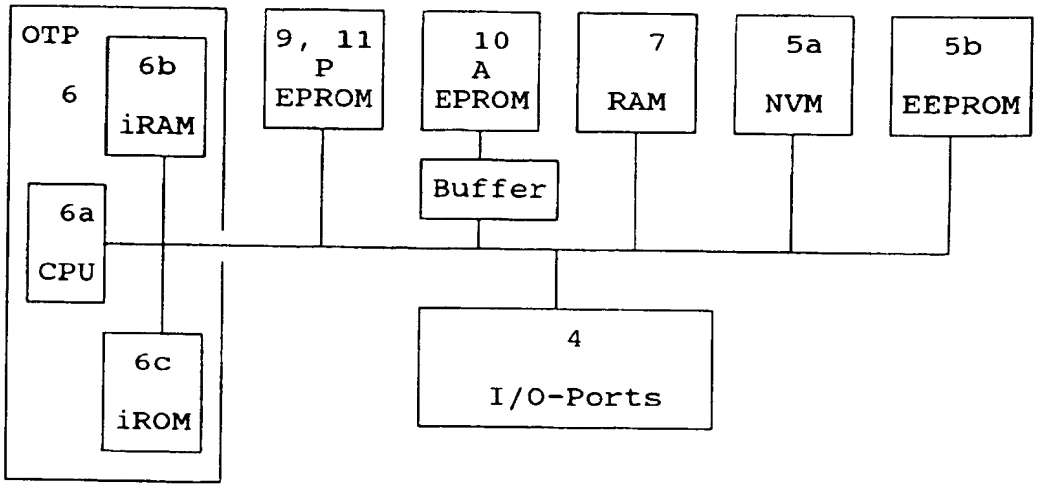

Fig. 2

BNSDOCID: <EP_____0762338A2_I_>

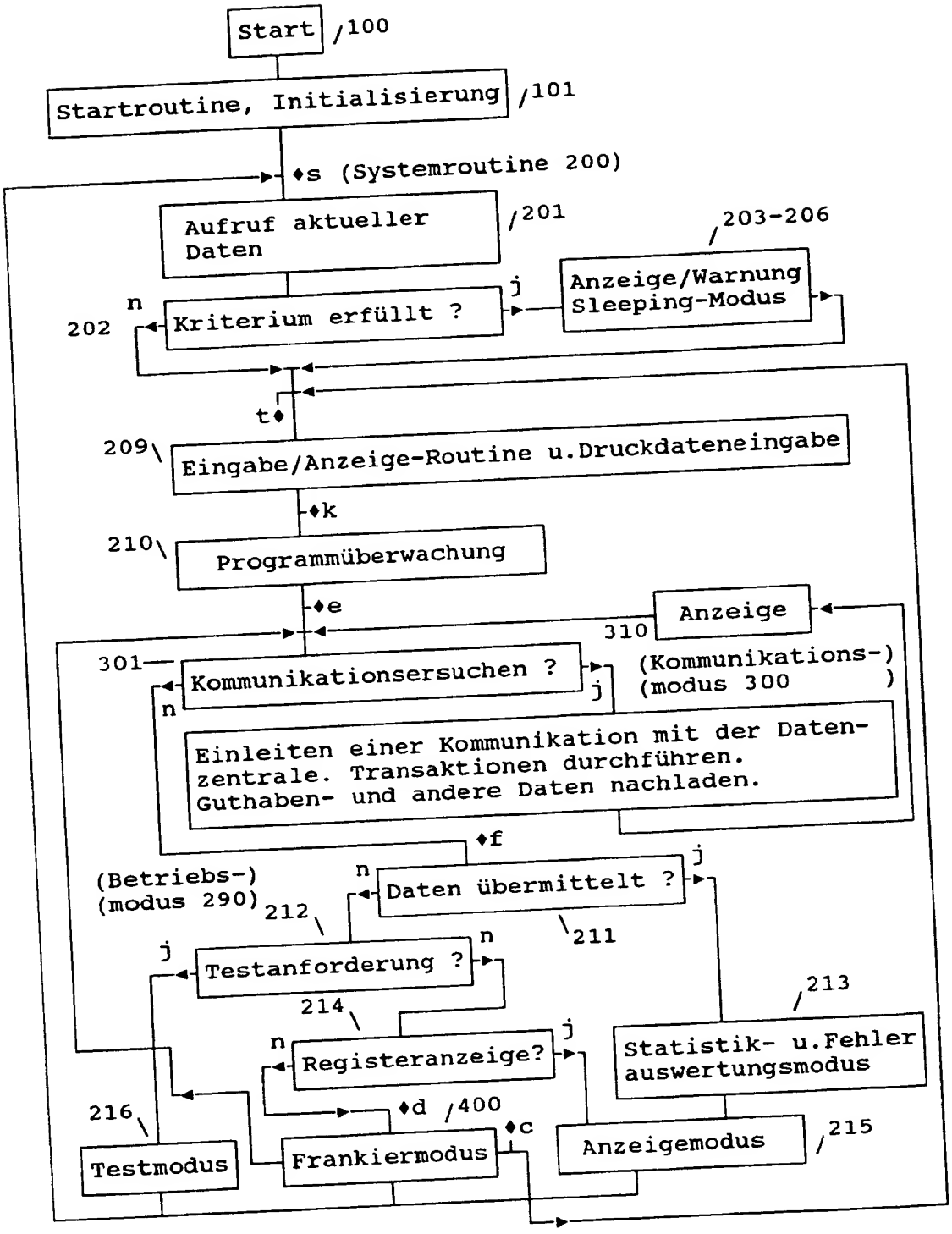

Fig. 3

BNSDOCID: <EP_____0762338A2_I_>

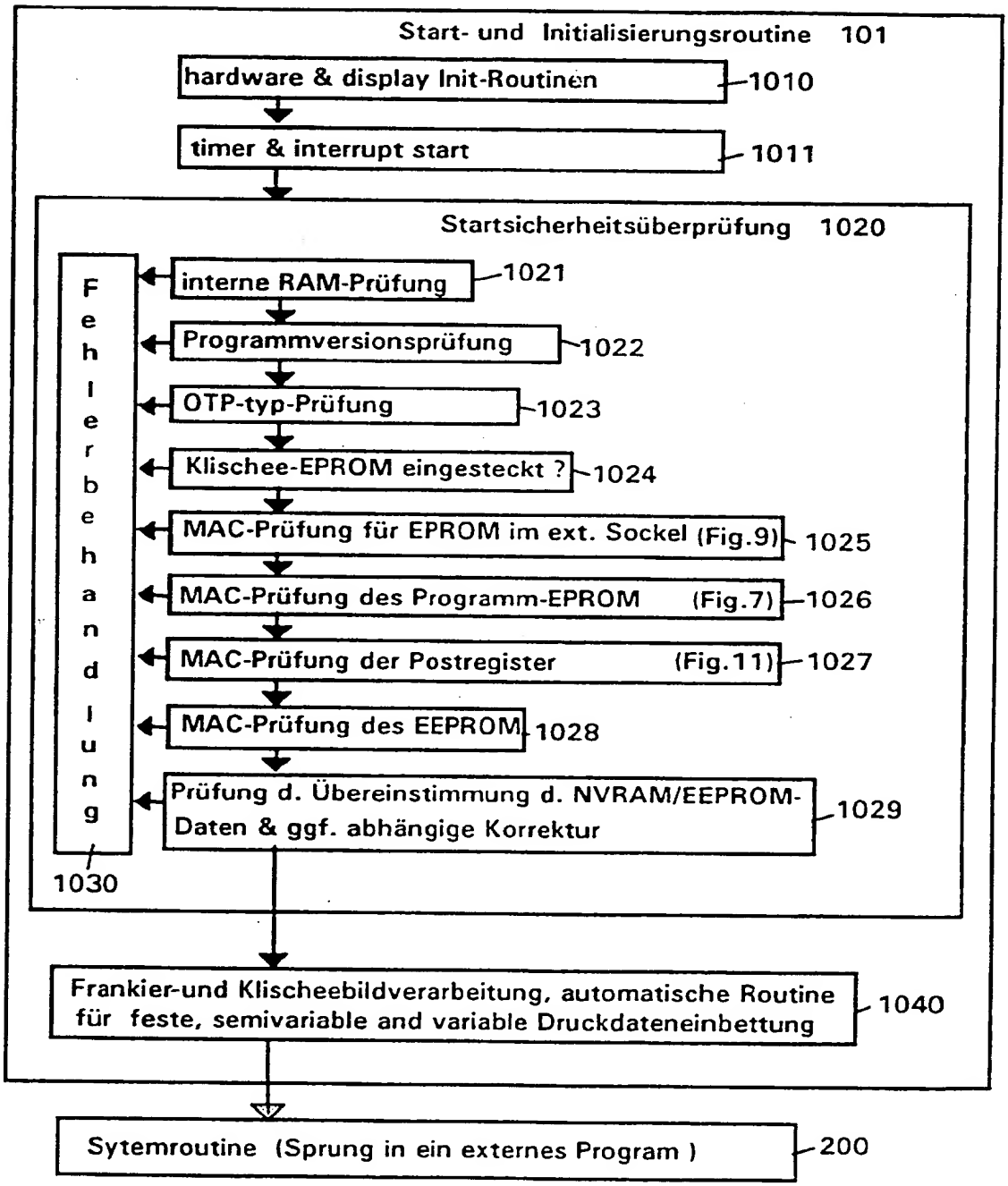

Fig. 4

BNSDOCID: <EP_____0762338A2_I_>

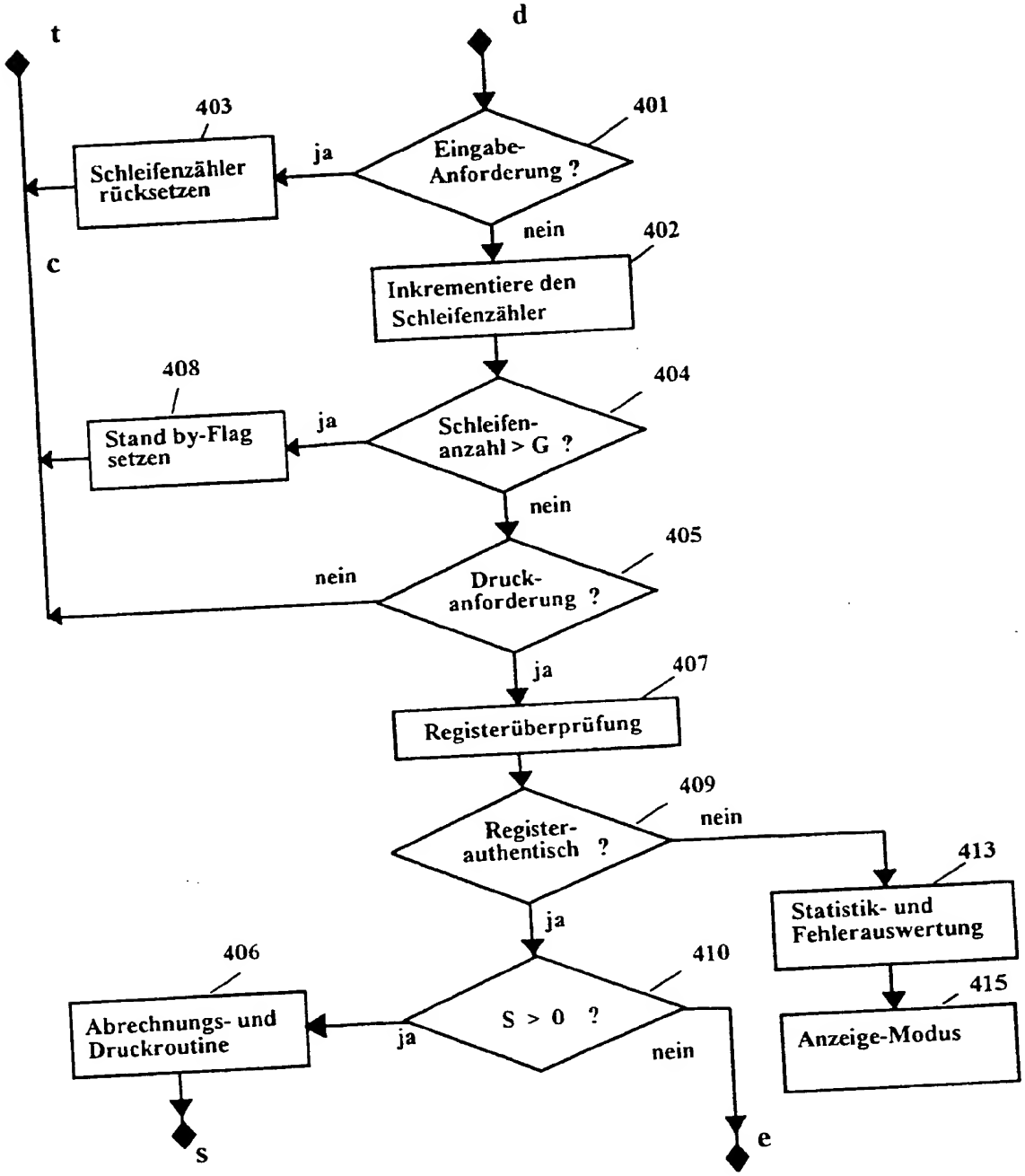

Fig. 5

BNSDOCID: <EP_____0762338A2_I_>

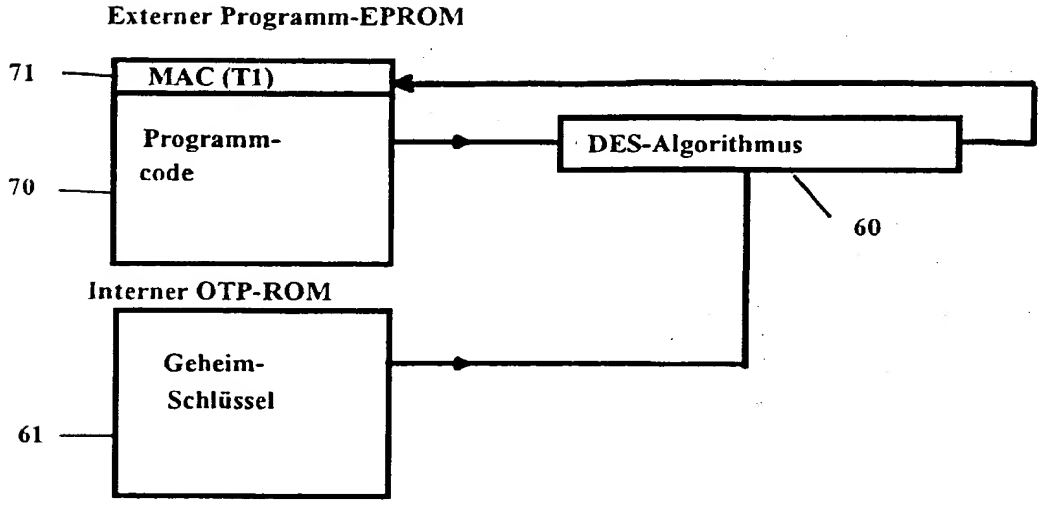

Fig. 6

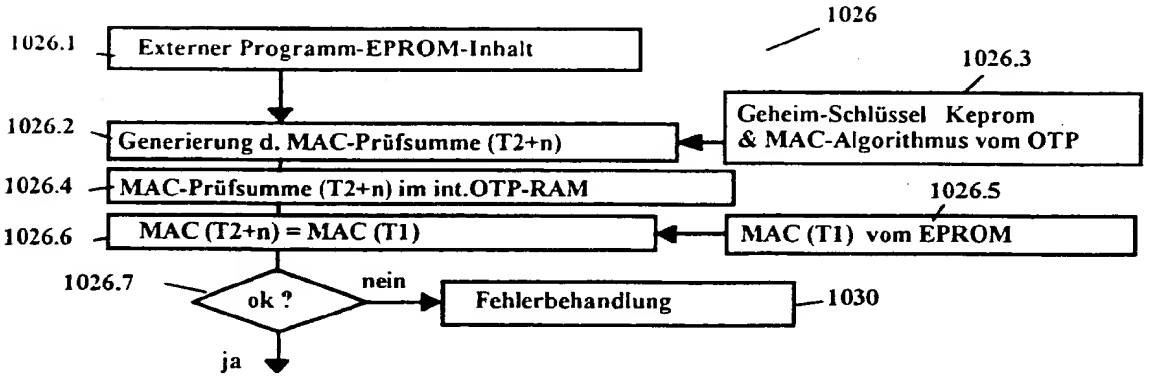

Fig. 7

BNSDOCID: <EP_____0762338A2_I_>

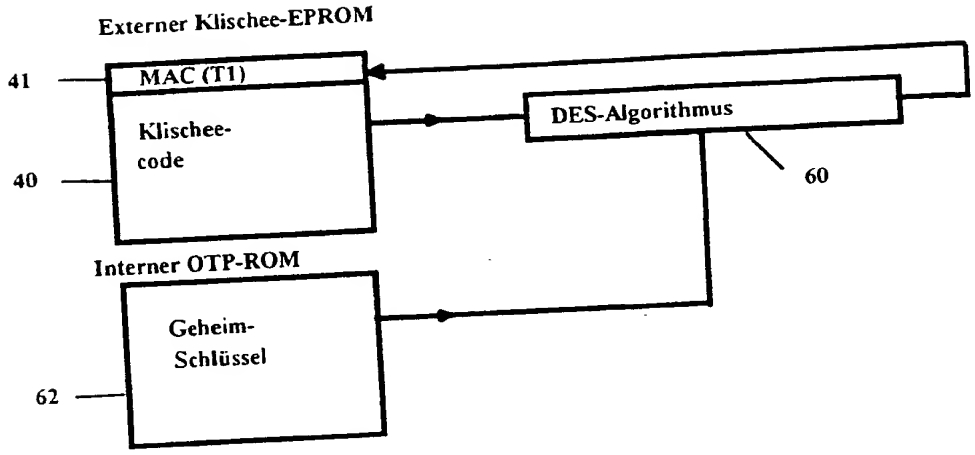

Fig. 8

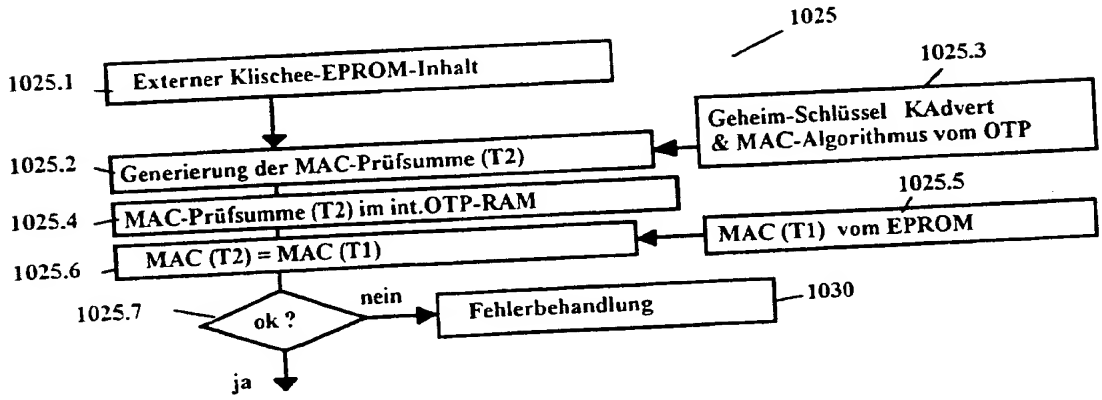

Fig. 9

BNSDOCID <EP_____0762338A2_I_>

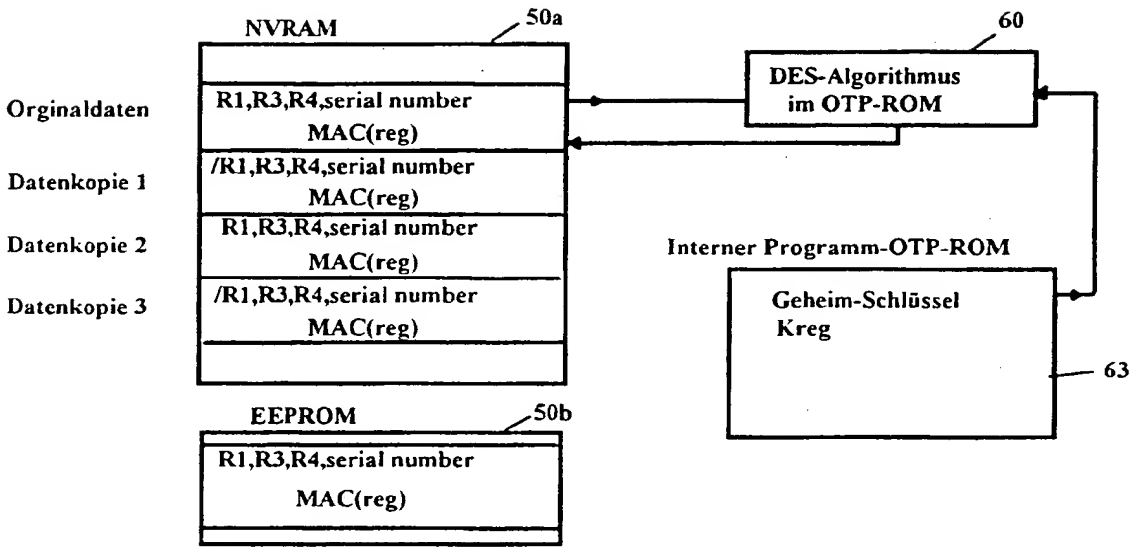

Fig. 10

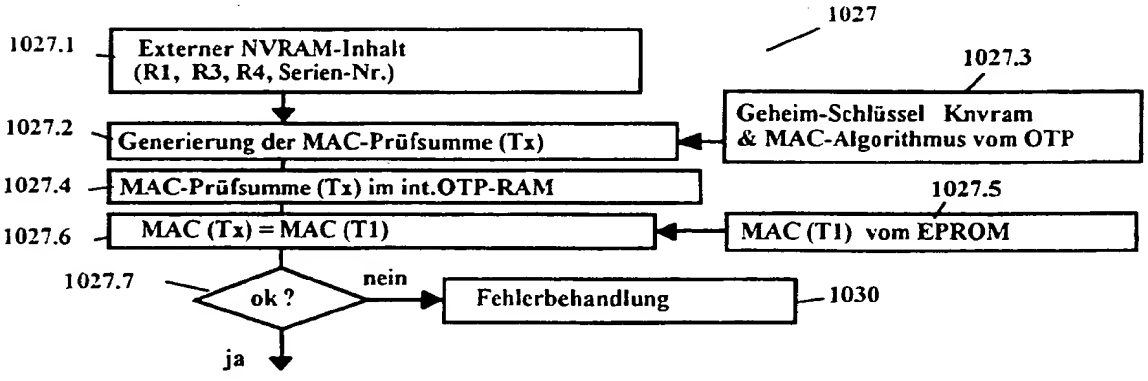

Fig. 11

BNSDOCID: <EP_____0762338A2_I_>

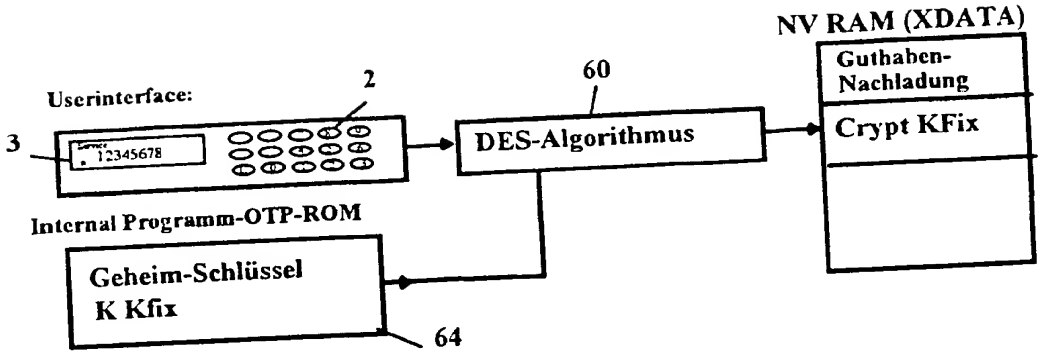

Fig. 12

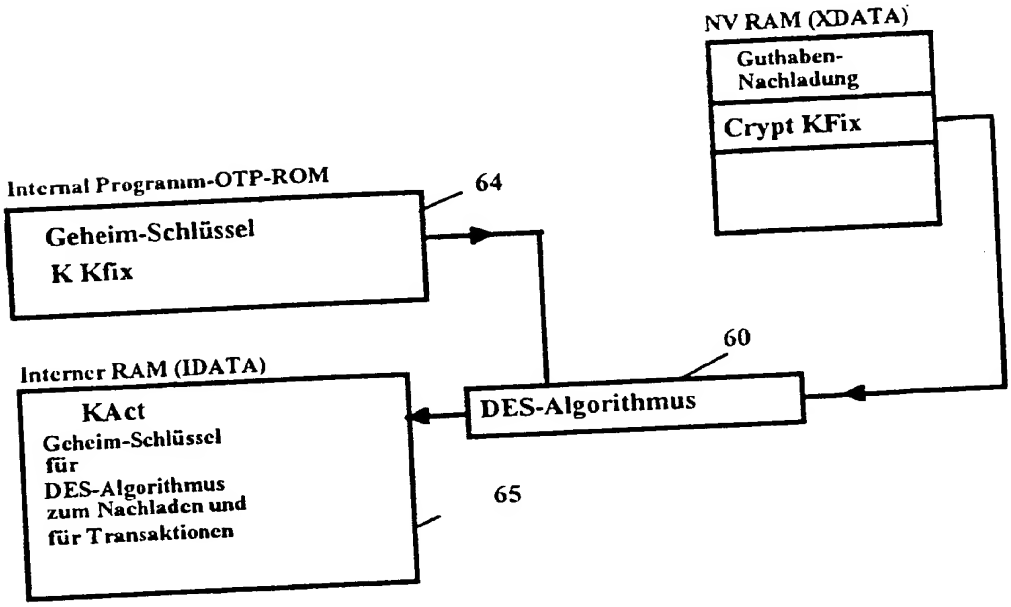

Fig. 13

BNSDOCID: <EP_____0762338A2_I_>

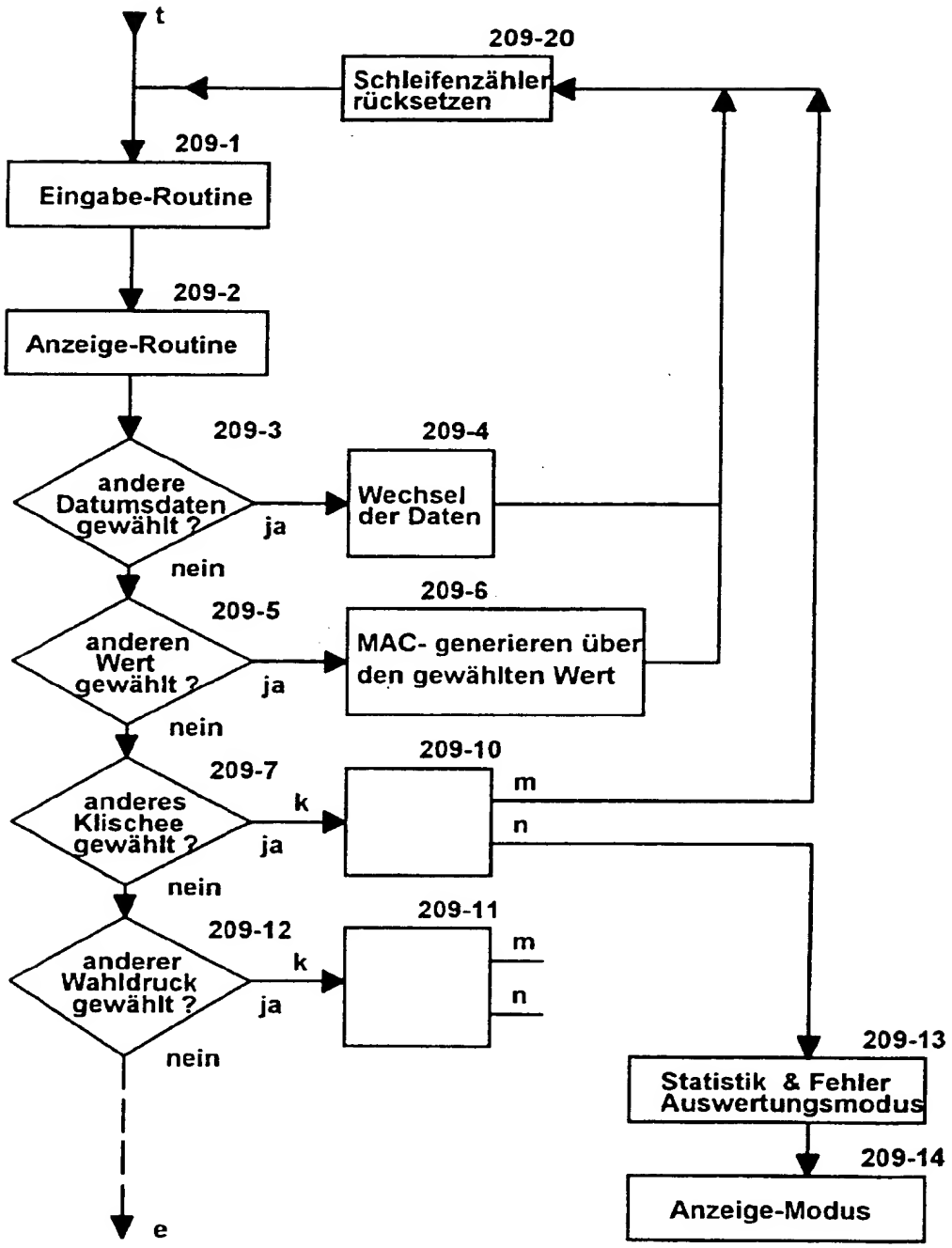

Fig. 14

BNSDOCID: <EP_____0762338A2_I_>

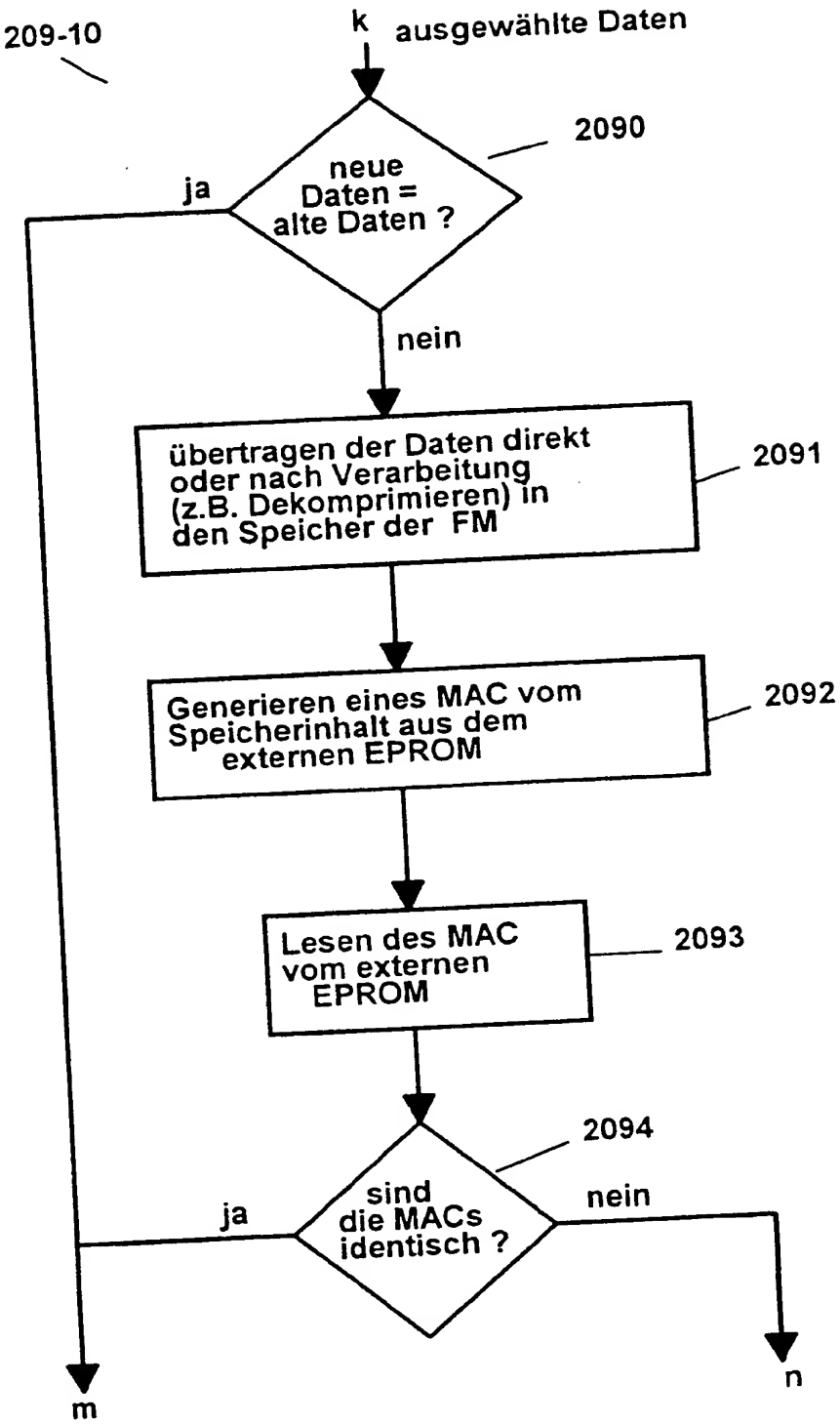

Fig. 15

BNSDOCID <EP_____0762338A2_I_>

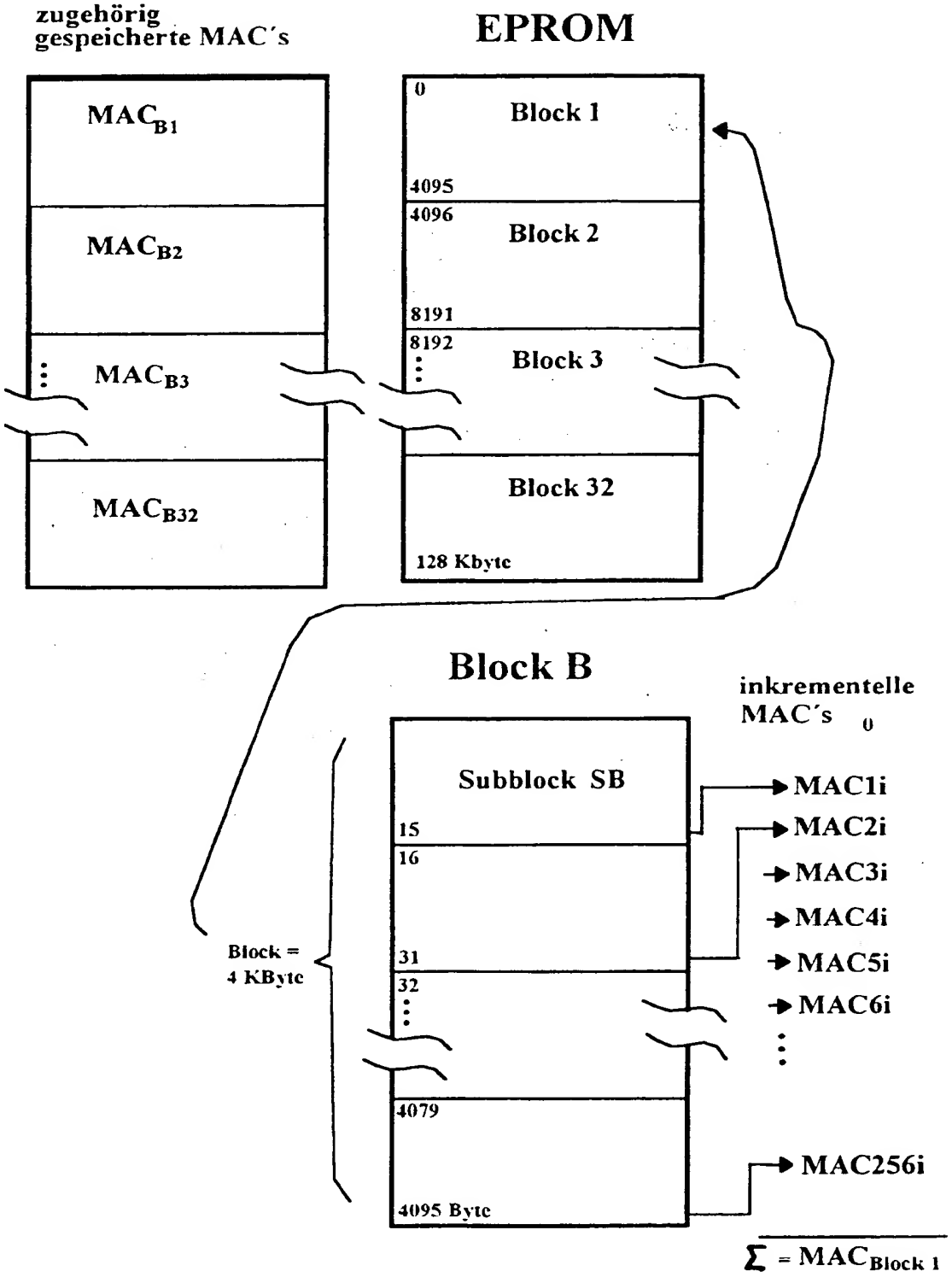

Fig. 16

BNSDOCID: <EP_____0762338A2_I_>

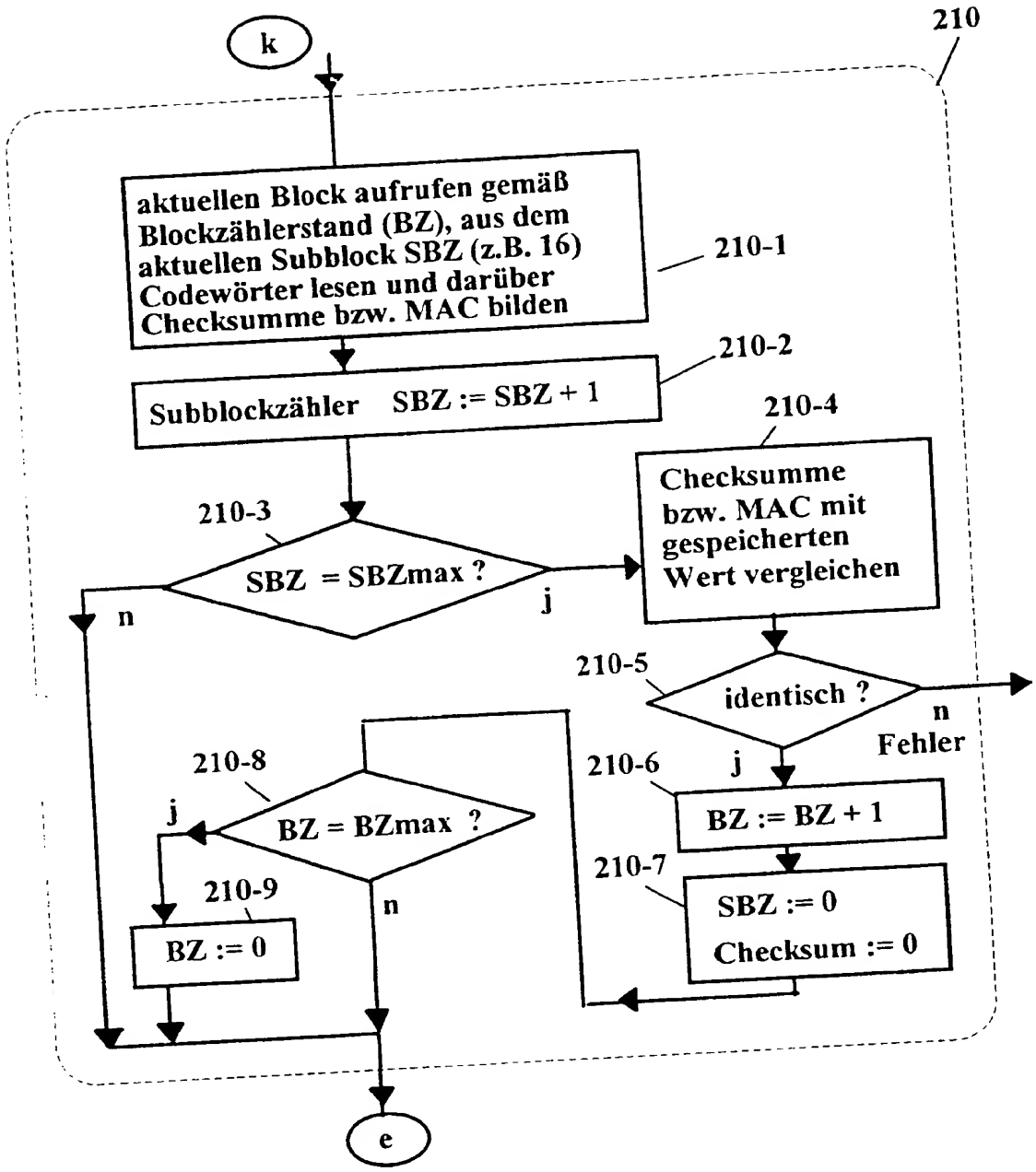

Fig. 17

BNSDOCID <EP_____0762338A2_I_>

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 762 338 A3

(12) EUROPÄISCHE PATENTANMELDUNG

(88) Veröffentlichungstag A3:
26.01.2000 Patentblatt 2000/04

(43) Veröffentlichungstag A2:
12.03.1997 Patentblatt 1997/11

(21) Anmeldenummer: **96250192.0**

(22) Anmeldetag: **06.09.1996**

(51) Int. Cl.[7]: **G07B 17/04**

(84) Benannte Vertragsstaaten:
CH DE FR GB IT LI

(30) Priorität: **08.09.1995 DE 19534530**

(71) Anmelder:
Francotyp-Postalia Aktiengesellschaft & Co.
16547 Birkenwerder (DE)

(72) Erfinder:
- **Berthold, Arndt**
  10369 Berlin (DE)
- **Zarges, Olav A.**
  13353 Berlin (DE)

(54) Verfahren zur Absicherung von Daten und Programmcode einer elektronischen Frankiermaschine

(57) Die Erfindung betrifft ein Verfahren zur Absicherung von Daten und Programmcode einer elektronischen Frankiermaschine gegen Manipulation mit einem Mikroprozessor in einer Steuereinheit der Frankiermaschine zur Ausführung von Schritten für eine Start- und Initialisierungsroutine und nachfolgender Systemroutine mit einer Möglichkeit in einen Kommunikationsmodus mit einer entfernten Datenzentrale einzutreten sowie weiteren Eingabeschritten, um in einen Frankiermodus einzutreten von dem nach Ausführung einer Abrechnungs- und Druckroutine in die Systemroutine zurückverzweigt wird, umfassend

a) eine Startsicherheitsüberprüfung (1020) im Rahmen einer Start- und Initialisierungsroutine (101) vor einer sicheren Druckdatenaufrufroutine (1040) und der nachfolgenden Systemroutine (200) zur Feststellung der Gültigkeit eines Programm-Codes und/oder von Daten im vorbestimmten Speicherplatz und eines zugehörigen MAC (MESSAGE AUTHENTIFICATION CODE), welche im selben Speichermittel gespeichert vorliegen, wobei die Überprüfung auf gültigen Programm-Code und/oder auf Gültigkeit der Daten mittels eines ausgewählten Prüfsummenverfahrens innerhalb eines OTP-Prozessors (ONE TIME PROGRAMMABLE) durchgeführt wird, der intern die entsprechenden Programmteile enthält und

b) eine Überführung der Frankiermaschine in die vorgenannte Systemroutine (200) bei Gültigkeit der Daten oder Überführung der Frankiermaschine in einen ersten Modus, wenn die Daten ungültig sind bzw. ein spezifisches Manipulationskriterium erfüllt ist, durch Schritte zum Verhindern des Frankierens bzw. Sperrens der Frankiermaschine (1030) und/oder Schritte zum Verhindern einer weiteren Programmausführung bzw. einer vom OTP-Prozessor nach extern führenden Programmverzweigung im Rahmen vorgenannter Systemroutine (200).

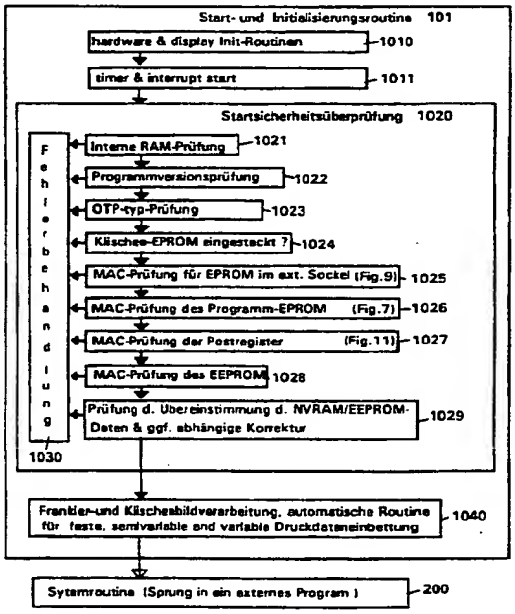

Fig. 4

EP 0 762 338 A3

Europäisches Patentamt

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 96 25 0192

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (Int.Cl.6)
Y A	EP 0 281 225 A (HEWLETT PACKARD CO) 7. September 1988 (1988-09-07) * Seite 2, Spalte 34 - Seite 3, Spalte 6 * * Seite 16, Spalte 19 - Spalte 58 * * Ansprüche 1-3,7; Abbildung 6 * ---	1,3-5, 13-15 6-10,12	G07B17/04
Y A	DE 43 44 476 A (FRANCOTYP POSTALIA GMBH) 22. Juni 1995 (1995-06-22) * Seite 4, Spalte 30 - Spalte 65 * * Ansprüche 1-3,7,10 * ---	1,3-5, 13-15 6-10,12	
D,A	DE 41 29 302 A (LEMBENS HELMUT) 4. März 1993 (1993-03-04) * Spalte 6, Zeile 28 - Zeile 58 * * Ansprüche 11,12; Abbildung 1 * ---	11	
A	US 4 726 025 A (SPLETT KATHERINE A ET AL) 16. Februar 1988 (1988-02-16) * Ansprüche 1-4 * ---	2	
A	PATENT ABSTRACTS OF JAPAN vol. 012, no. 480 (P-801), 15. Dezember 1988 (1988-12-15) & JP 63 196936 A (NEC CORP), 15. August 1988 (1988-08-15) * Zusammenfassung * -----	1,13,14	RECHERCHIERTE SACHGEBIETE (Int.Cl.6) G07B G06F G07F H04L

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
DEN HAAG	3. Dezember 1999	Reule, D

KATEGORIE DER GENANNTEN DOKUMENTE

X : von besonderer Bedeutung allein betrachtet
Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie
A : technologischer Hintergrund
O : nichtschriftliche Offenbarung
P : Zwischenliteratur

T : der Erfindung zugrunde liegende Theorien oder Grundsätze
E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist
D : in der Anmeldung angeführtes Dokument
L : aus anderen Gründen angeführtes Dokument

& : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument

EPO FORM 1503 03.82 (P04C03)

BNSDOCID <EP_____0762338A3_I_>

ANHANG ZUM EUROPÄISCHEN RECHERCHENBERICHT ÜBER DIE EUROPÄISCHE PATENTANMELDUNG NR. EP 96 25 0192

In diesem Anhang sind die Mitglieder der Patentfamilien der im obengenannten europäischen Recherchenbericht angeführten Patentdokumente angegeben.
Die Angaben über die Familienmitglieder entsprechen dem Stand der Datei des Europäischen Patentamts am
Diese Angaben dienen nur zur Unterrichtung und erfolgen ohne Gewähr.

03-12-1999

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
EP 0281225 A	07-09-1988	DE 3889561 D	23-06-1994
		DE 3889561 T	01-09-1994
		JP 2675806 B	12-11-1997
		JP 63225840 A	20-09-1988
		US 4933969 A	12-06-1990
DE 4344476 A	22-06-1995	EP 0660269 A	28-06-1995
		US 5671146 A	23-09-1997
		US 5805711 A	08-09-1998
DE 4129302 A	04-03-1993	WO 9305482 A	18-03-1993
		EP 0604464 A	06-07-1994
US 4726025 A	16-02-1988	US RE33461 E	27-11-1990
JP 63196936 A	15-08-1988	KEINE	

EPO FORM P0461

Für nähere Einzelheiten zu diesem Anhang : siehe Amtsblatt des Europäischen Patentamts, Nr.12/82

BNSDOCID: <EP_____0762338A3_I_>

Method for securing data and progam code of an electronic franking machin

Patent number: EP0762338
Publication date: 1997-03-12
Inventor: BERTHOLD ARNDT (DE); ZARGES OLAV A (DE)
Applicant: FRANCOTYP POSTALIA AG (DE)
Classification:
- international: G07B17/04
- european: G07B17/00G
Application number: EP19960250192 19960906
Priority number(s): DE19951034530 19950908

Also published as:
EP0762338 (A3)
DE19534530 (A

Cited documents:
EP0281225
DE4344476
DE4129302
US4726025
JP63196936

Report a data error he

Abstract of **EP0762338**

A summation is used for a starting check (1020) in the frame of the starting and initialisation routine (101) that runs before the printed date routine (1040) and the following system routine (200) for validating the programme code and certain data. The appropriate MAC is entered and the above routine is performed using a summation testing method from the OTP processor, with its algorithm and key. The franking machine is run in the same routine (200) of a similar validation is made, and the process is repeated for various manipulation or handling modes.

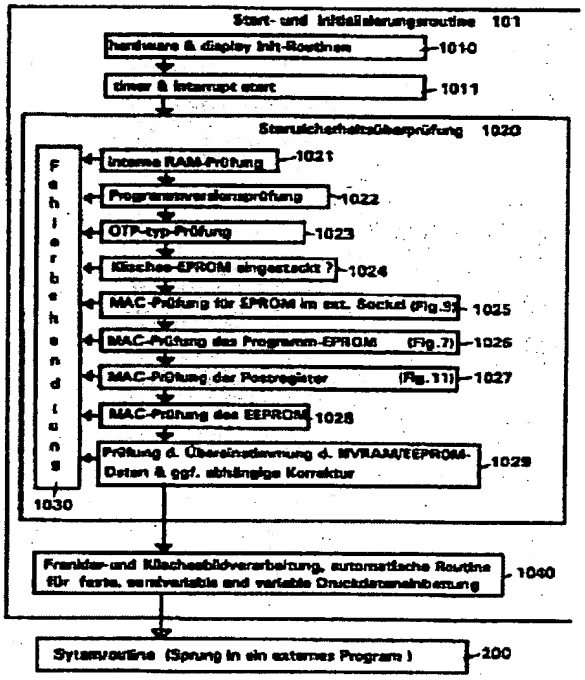

Fig. 4

Data supplied from the *esp@cenet* database - Worldwide

DOCKET NO: GTP/US 3183
SERIAL NO: 09/917,541
APPLICANT: Reisinger et al.

LERNER AND GREENBERG P.A.
P.O. BOX 2480
HOLLYWOOD, FLORIDA 33022
TEL. (954) 925-1100